Arcserve RHA®

Guida per l'amministratore

r16.5

La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da Arcserve in qualsiasi momento.

Questa Documentazione non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di Arcserve. Questa Documentazione è di proprietà di Arcserve e non potrà essere divulgata o utilizzata se non per gli scopi previsti in (i) uno specifico contratto tra l'utente e Arcserve in merito all'uso del software Arcserve cui la Documentazione attiene o in (ii) un determinato accordo di confidenzialità tra l'utente e Arcserve.

Fermo restando quanto enunciato sopra, se l'utente dispone di una licenza per l'utilizzo dei software a cui fa riferimento la Documentazione avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di Arcserve.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a Arcserve per iscritto che tutte le copie anche parziali del prodotto sono state restituite a Arcserve o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, LA DOCUMENTAZIONE VIENE FORNITA "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO ARCSERVE SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DEL GOODWILL O DI DATI, ANCHE NEL CASO IN CUI ARCSERVE VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è Arcserve.

Questa Documentazione è fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

Copyright © 2014 Arcserve (USA), LLC e affiliate. Tutti i diritti riservati. Tutti i marchi, le denominazioni sociali, i marchi di servizio e i logo citati in questa pubblicazione sono di proprietà delle rispettive società.

Riferimenti ai prodotti Arcserve

Questo documento fa riferimento ai seguenti prodotti Arcserve:

- Arcserve® Replication
- Arcserve® High Availability (HA)
- Arcserve® Assured Recovery®
- Arcserve® Content Distribution

Modifiche apportate alla documentazione

Di seguito sono riportati gli aggiornamenti apportati alla documentazione dall'ultima release.

- Aggiornamento contenente commenti e suggerimenti degli utenti, correzioni e altre modifiche minori per migliorare le modalità di utilizzo e il funzionamento del prodotto o la documentazione stessa.
- È stata aggiunta la sezione Scenari cloud Replication e High Availability. (a pagina 89)
- È stata aggiunta la sezione Gestione dei cluster. (a pagina 353)
- È stato aggiunto un nuovo argomento alla sezione Esecuzione del processo di replica denominato Modifica della configurazione di scenario (a pagina 240) contenente le informazioni relative alla modifica di uno scenario in esecuzione.
- È stata aggiunto un nuovo argomento sull'uso dell'utilità NAT.

Come contattare Arcserve

Il team del Supporto tecnico di Arcserve offre un set di risorse per la risoluzione dei problemi tecnici e l'accesso a importanti informazioni sul prodotto.

https://www.arcserve.com/support

Con il Supporto tecnico di Arcserve:

- È possibile consultare direttamente la stessa libreria di informazioni condivisa internamente dagli esperti del Supporto tecnico di Arcserve. Questo sito fornisce l'accesso ai documenti della Knowledge Base (KB). Da qui, è possibile cercare e trovare facilmente gli articoli della Knowledge Base relativi al prodotto e contenenti le soluzioni testate sul campo a molti problemi principali e comuni.
- È possibile utilizzare il collegamento alla Chat in tempo reale per avviare una conversazione in tempo reale con il team di Supporto tecnico di Arcserve. Con la Chat in tempo reale, è possibile ottenere risposte immediate alle proprie domande e preoccupazioni, mantenendo al contempo l'accesso al prodotto.
- È possibile partecipare alla Arcserve Global User Community per porre domande e rispondere, condividere suggerimenti e consigli, discutere su procedure consigliate e partecipare a discussioni con i propri colleghi.
- È possibile aprire un ticket di supporto. Quando si apre un ticket di supporto in linea, si verrà contattati da uno degli esperti nell'area del prodotto per il quale si richiede il supporto.

È possibile accedere ad altre risorse utili relative al prodotto Arcserve.

Commenti e suggerimenti sulla documentazione dei prodotti

Per eventuali commenti o domande sulla documentazione di prodotto Arcserve, si prega di contattarci.

Sommario

Capitolo 1: Introduzione 15

Informazioni sulla guida 15
Visualizzazione della documentazione correlata 16
Server applicazioni e database supportati 17
Concetti di Arcserve RHA 18
- Funzionamento della sincronizzazione 18
- Funzionamento della replica 21
- Funzionamento del recupero 22
- Funzionamento del ripristino dei dati 23
- Funzionamento della sospensione della replica 23
- Funzionamento di High Availability 24
- Funzionamento di Assured Recovery per file server 25
- Limitazioni 25

Componenti di Replication e High Availability 25
- Servizio di controllo 25
- Modulo 26
- Centro di gestione 27
- PowerShell 28
- Arcserve RHA per il cluster di failover Microsoft 28

Modalità di distribuzione di Arcserve RHA 28

Capitolo 2: Esplorazione della Gestione 29

Accesso al Centro di gestione 30
Collegamenti per l'accesso al supporto tecnico e alla community 32
Esplorazione della schermata Gestione di Arcserve RHA 34
- Riquadri della schermata Gestione 35

Visualizzazione e organizzazione della schermata Gestione 37
- Opzioni di visualizzazione 37
- Personalizzazione della visualizzazione scenario 37
- Riorganizzazione dei riquadri 38

Barre degli strumenti 41
- Barra degli strumenti standard 42
- Barra degli strumenti Visualizzazione 45

Registrazione licenze di Arcserve RHA 45

Capitolo 3: Creazione di scenari Replication e High Availability 47

Creazione di uno scenario di replica di file server 47
Creazione di scenari Arcserve Central Host-Based VM Backup 57
Verifica dei prerequisiti 59
Creazione dello scenario 59
Verifica dello scenario 66
Creazione di un nuovo scenario HA per file server 66
Uso dei Gruppi di scenari 73
Creazione di un gruppo di scenari 74
Impostazione delle proprietà del gruppo 75
Abilitazione della gestione di gruppi di scenari 76
Esecuzione di un gruppo di scenari 79
Interruzione di un gruppo di scenari 80
Utilizzo dei modelli 80
Creazione di un nuovo modello 80
Creazione di un nuovo scenario utilizzando un modello esistente 84
Gestione degli host che utilizzano periferiche NAT 86
Configurare l'utilità NAT 87
Creazione di uno scenario con l'utilità NAT 87

Capitolo 4: Creazione di scenari cloud Replication e High Availability 89

Panoramica 90
Failover sistema completo EC2 91
Utilizzo degli scenari cloud High Availability di Arcserve RHA 93
Utilizzo degli scenari Arcserve RHA Replication in ambiente cloud 94
Replica su cloud 95
Pannello Visualizzazione cloud 96
Configurazione del proxy Web per la connessione al servizio cloud 101
Aggiunta di un nuovo account cloud 102
Modifica dell'area AWS predefinita 104
Aggiornamento delle informazioni dell'account cloud 104
Eliminazione di un account cloud 104
Creazione di una nuova istanza di replica EC2 105
Avvio di un'istanza di replica EC2 111
Interruzione di un'istanza di replica EC2 111
Eliminazione di un'istanza di replica EC2 112
Creazione di un nuovo scenario High Availability per sistemi completi EC2 112
Creazione di un nuovo scenario di replica dei dati su EC2 120
Esecuzione e sincronizzazione di uno scenario Replication o High Availability per i dati di sistemi completi EC2 124
Esecuzione dell'avanzamento per uno scenario High Availability per sistemi completi EC2 125

Esecuzione del recupero mediante una replica EC2 di failover 126

Capitolo 5: Esecuzione del processo di replica 127

Avvio della replica 127
Modalità di esecuzione 130
Esecuzione di uno scenario mediante un server proxy 130
Interruzione della replica 131
Sincronizzazione dei server master e replica 131
Funzionamento della sincronizzazione non in linea 133
Autenticazione host 141
Abilitazione della replica multitenancy 141
Procedura di abilitazione della replica multitenancy 142
Chiusura e apertura della Gestione durante la replica 147
Sospendi replica 148
Sospensione manuale della replica 149
Ripresa della replica in seguito a una sospensione manuale 150
Pianificazione della sospensione replica automatica 150
Esecuzione di uno scenario in modalità di valutazione 153

Capitolo 6: Monitoraggio della replica 155

Pagina con informazioni introduttive 155
Gestione 155
Modalità di controllo per scenari multipli 156
Informazioni sullo stato 156
Statistiche live 157
Visualizzazione eventi 164
Visualizzazione di eventi in una finestra separata 164
Visualizzazione di eventi in entrata 164
Copia di eventi per l'utilizzo con altri programmi 165
Filtro eventi 165
Rapporti di Arcserve RHA 166
Visualizzazione di un rapporto 167
Eliminazione di rapporti 168
Rapporti di sincronizzazione 168
Rapporti di replica 169
Per aprire un rapporto su uno scenario precedente, procedere come segue: 169
Rapporti delle differenze 169
Rapporti della modalità valutazione 170

Capitolo 7: Modifica e gestione di scenari e host 171

Definizione dei server master e di replica 172
Aggiunta di server di replica supplementari 173
Selezione di directory master e del relativo contenuto per la replica 174
Modifica dei nomi delle directory 177
Rimozione delle Directory principali master 177
Filtro dei file nelle directory master 178
Includi file 179
Escludi file 182
Sincronizzazione chiavi di registro 184
Attivazione dell'opzione Sincronizzazione registro 184
Selezione delle chiavi di registro per la sincronizzazione 186
Selezione del nome e della posizione di archiviazione per le chiavi di registro sincronizzate 187
Rilevamento automatico dei file di database per tutti i database 189
Selezione di directory principali di replica 191
Propagazione delle directory principali master a più host di replica 193
Operazioni dello scenario 194
Salvataggio degli scenari 195
Rimozione di scenari 195
Esportazione di scenari 196
Importazione di scenari 197
Manutenzione degli host 197
Informazioni sull'opzione di manutenzione host 198
Preparazione degli host per le procedure di manutenzione 199

Capitolo 8: Impostazione delle proprietà 201

Configurazione delle proprietà di uno scenario 201
Nozioni fondamentali sulle proprietà dello scenario 202
Proprietà generali 202
Proprietà di replica 203
Proprietà Notifica evento 208
Proprietà di gestione rapporti 210
Pianificazione della sincronizzazione 211
Impostazione di una pianificazione per la sincronizzazione automatica 213
Esclusione di date dalla sincronizzazione pianificata 214
Impostazione di pianificazioni avanzate 214
Impostazione delle proprietà del server master e di replica 215
Configurazione delle proprietà del server master o di replica 216
Nozioni fondamentali sulle proprietà master 217
Nozioni fondamentali sulle proprietà del server di replica 224
Pianificazione del limite di larghezza di banda 237

Propagazione dei valori delle proprietà 238
Modifica della configurazione durante l'esecuzione di uno scenario 240
Protezione dello stato del sistema 241
Come configurare la Protezione stato del sistema 243
Modifica della protezione dello stato del sistema per lo scenario 248
Ripristino dei dati relativi allo stato del sistema 249
Miglioramenti della riga di comando per la protezione dello stato del sistema 250
Informazioni aggiuntive sullo stato del sistema 250

Capitolo 9: Recupero di dati e server 251

Processo di ripristino dei dati 251
Ripristino di dati perduti dal server di replica 252
Impostazione di segnalibri 254
Ripristino dei dati 255

Capitolo 10: Avanzamento e regressione 259

Avanzamento 259
Flusso di lavoro di avanzamento 259
Avvio dell'avanzamento 260
Regressione 262
Flusso di lavoro di regressione 262
Avvio della regressione 263
Recupero del server attivo 265
Ripristino del server attivo mediante la Gestione 265
Ripristino del server attivo senza utilizzare Gestione 267
Nozioni fondamentali sul sistema High Availability e sulle procedure di avanzamento e regressione 270
Impostazione delle proprietà High Availability 271
Configurazione delle proprietà High Availability 272
Nozioni fondamentali sulle proprietà High Availability 273
Host attivi e in stand-by 285
Reindirizzamento con IP di spostamento 285

Capitolo 11: Protezione del Servizio di controllo 295

Nozioni fondamentali sugli scenari Servizio di controllo 295
Creazione di scenari High Availability per il Servizio di controllo 298
Apertura della Gestione per l'utilizzo dello scenario HA del Servizio di controllo 302
Inversione dei ruoli tra il Servizio di controllo attivo e in stand-by 303
Avvio manuale dell'avanzamento del Servizio di controllo attivo 304
Processi Avanzamento e Scenario precedente 305
Regressione dei ruoli del Servizio di controllo 307

Capitolo 12: Verifica Assured Recovery 309

Informazioni su Assured Recovery 309
Creazione di uno scenario di verifica Assured Recovery 311
Configurazione delle proprietà Assured Recovery 314
Impostazione delle proprietà di Assured Recovery 316
Limiti della verifica Assured Recovery 319
Esecuzione di una verifica Assured Recovery 319
Esecuzione della verifica Assured Recovery in modalità non pianificata 320
Esecuzione della verifica Assured Recovery in modalità non pianificata 322

Capitolo 13: Utilizzo di snapshot VSS 327

Creazione automatica di snapshot VSS 327
Impostazione della creazione di snapshot 328
Nozioni fondamentali sulle proprietà delle snapshot VSS 331
Visualizzazione e gestione delle snapshot 331
Visualizzazione di snapshot 331
Gestione delle snapshot 332

Capitolo 14: Utilizzo della soluzione Content Distribution 335

Nozioni fondamentali sulla soluzione Content Distribution 335
Creazione scenario Distribuzione contenuto (CD) 337

Capitolo 15: Gestione utenti 343

Funzionamento della protezione delegata 343
Considerazioni sui diritti di accesso 344
Attività preliminari per la gestione utenti 344
Creazione di un gruppo di utenti 344
Selezione del gruppo iniziale 345
Impostazione di un gruppo utenti 345
Come gestire gli utenti 346
Delega dei diritti 346
Impostazione dei diritti degli utenti 348
Impostazione del gruppo utente con privilegi 348

Capitolo 16: Gestione dei servizi 349

Gestione servizi 350

Capitolo 17: Gestione dei cluster 353

Introduzione ai miglioramenti apportati al cluster Windows 2008 353
Funzionamento del supporto migliorato per i cluster Arcserve RHA....354
Distribuzione dei componenti Arcserve RHA per il supporto cluster....354
Installazione di Arcserve RHA per i cluster di failover Microsoft 355
Avvio di Arcserve RHA per i cluster di failover Microsoft 355
Azioni della console....356
Replica di dati cluster e gestione di risorse....363
Apertura di un cluster 363
Ricerca di cluster 364
Creazione di una nuova risorsa disco....365
Aggiunta di risorse disco ad applicazioni 365
Gestione delle licenze 366
Ricerca di eventi....366

Capitolo 18: Creazione ed esecuzione degli script definiti dall'utente 367

Funzionamento degli script definiti dall'utente con Arcserve RHA....368
Proprietà degli script definiti dall'utente 368
Esecuzione degli script definiti dall'utente da Proprietà scenario 369
Esecuzione di script definiti dall'utente da Proprietà master 369
Esecuzione di script definiti dall'utente da Proprietà di replica....371
Esecuzione degli script definiti dall'utente da Proprietà delle attività pianificate.....373
Esecuzione dello script definito dall'utente da Proprietà High Availability 375
Specificare uno script definito dall'utente in Proprietà 376
Uso dello script di risoluzione dei problemi....377

Capitolo 19: Configurazione dell'utilità NAT per RHA per impostazioni di rete diverse 379

Esempio 1: Master protetti da firewall chiuso 380
Creazione di uno scenario HA per sistemi completi....382
Esecuzione del ripristino bare metal da un punto di ripristino....384
Esecuzione del ripristino bare metal mediante la replica inversa 385
Esempio 2: Master protetti da firewall chiuso con un server proxy 387
Esempio 3: Dispositivo e CS protetti da firewall chiuso 390
Creazione di uno scenario HA per sistemi completi....391
Esecuzione del ripristino bare metal da un punto di ripristino....392
Esecuzione del ripristino bare metal mediante la replica inversa 392
Esempio 4: Servizio di controllo su WAN pubblica....393
Esempio 5: Master, dispositivo e Servizio di controllo protetti da firewall con inoltro alla porta....394

Appendice A: Risoluzione dei problemi di Arcserve RHA 397

Suggerimenti per la risoluzione dei problemi 397
Disco pieno 400
Rinnovo di un certificato SSL scaduto 402
Impossibile iniziare l'ascolto sulla porta/e 403
Aprire le porte necessarie per l'installazione remota e per la verifica del modulo 403
Modifica della porta del Servizio di controllo 404
Modifica della porta del modulo 405
Directory principali 406
Errore di creazione della copia shadow 407
Errore di creazione della copia shadow per il punto di montaggio VHD 408

Capitolo 1: Introduzione

Questa sezione contiene informazioni generali sui prodotti Arcserve Replication and High Availability (Arcserve RHA) e i relativi moduli. In essa vengono brevemente elencate nuove funzionalità, viene descritto il funzionamento Replication e High Availability, nonché il funzionamento dei vari moduli nel processo di replica.

Questa sezione contiene i seguenti argomenti:

Informazioni sulla guida (a pagina 15)
Visualizzazione della documentazione correlata (a pagina 16)
Server applicazioni e database supportati (a pagina 17)
Concetti di Arcserve RHA (a pagina 18)
Componenti di Replication e High Availability (a pagina 25)
Modalità di distribuzione di Arcserve RHA (a pagina 28)

Informazioni sulla guida

Questa guida contiene tutte le informazioni necessarie per la configurazione e l'esecuzione dell'applicazione Arcserve RHA. La guida descrive e fornisce istruzioni sulle modalità di esecuzione delle seguenti procedure:

- sincronizzazione
- replica e recupero dei dati
- procedure di controllo
- generazione di rapporti
- avanzamento dal server di produzione al server replica in stand-by e regressione
- protezione del Servizio di controllo.

Importante. Questa guida è valida per prodotti Replication, High Availability e Assured Recovery. All'interno del presente documento, il termine Arcserve RHA si riferisce a tutti i prodotti, salvo diversamente specificato.

Questa guida si concentra su soluzioni di Replication e High Availability per **file server**, ma fornisce anche informazioni su altri server applicazioni, server database e sulle soluzioni High Availability.

Per ulteriori istruzioni sugli scenari personalizzati per applicazioni specifiche, quali server Microsoft Exchange o SQL, si rimanda alla Guida operativa appropriata. Le guide operative più aggiornate per ogni applicazione sono disponibili sul sito del Supporto tecnico di Arcserve. Per ulteriori informazioni sulla visualizzazione delle Guide operative per applicazioni specifiche, si rimanda alla Documentazione correlata (a pagina 16).

Visualizzazione della documentazione correlata

La *Guida per l'amministratore di Arcserve RHA* è concepita per essere utilizzata con le seguenti guide supplementari´.

- *Guida all'installazione di Arcserve RHA - contiene informazioni relative all'installazione e alla configurazione di Arcserve RHA*
- *Guida ai comandi PowerShell di Arcserve RHA - contiene informazioni di riferimento sulla riga di comando*

In aggiunta, la guida operativa fornisce i dettagli, gli esempi e le impostazioni necessarie per utilizzare con successo il software in ambienti server applicazioni o database specifici. Le informazioni relative a Replication e High Availability vengono fornite in queste guide. (Nelle precedenti versioni di Arcserve RHA, venivano rilasciate guide separate per Replication (Disaster Recovery) e High Availability (HA)).

- *Guida operativa per Microsoft SQL Server di Arcserve RHA*
- *Guida operativa per Microsoft Exchange Server di Arcserve RHA*
- *Guida operativa per Microsoft SharePoint Server di Arcserve RHA*
- *Guida operativa per Microsoft Dynamics CRM di Arcserve RHA*
- *Guida operativa per Oracle Server di Arcserve RHA*
- *Guida operativa di Arcserve RHA per Microsoft IIS Server*
- *Guida operativa per BlackBerry Enterprise Server di Arcserve RHA*
- *Guida operativa per UNIX e Linux di Arcserve RHA*
- *Guida operativa per Virtualized Server Environments di Arcserve RHA*

Per ulteriori informazioni sull'integrazione di Arcserve RHA con Arcserve Backup, si rimanda alla *Guida all'integrazione di Arcserve Backup Arcserve RHA*nella documentazione di Arcserve Backup.

Per visualizzare le guide di Arcserve RHA:

1. Andare alla pagina del supporto Arcserve.
2. Fare clic su **Support and Learning** (Supporto e apprendimento) e quindi su **Documentazione** nell'elenco.

   Viene visualizzata la schermata Documentation.
3. Dall'elenco dei titoli dei documenti, fare clic sul collegamento di download accanto al documento che si desidera visualizzare.

Server applicazioni e database supportati

Le funzionalità Replication e High Availability sono personalizzate per i seguenti server applicazioni e database su Windows a 32 e a 64 bit:

- Microsoft File Server -- protezione per qualsiasi applicazione o tipo di dati, incluso database, purché la piattaforma OS e il file system siano supportati.
- Microsoft Exchange Server -- protezione per i server Exchange
- Microsoft SharePoint Server -- Protezione per i server SharePoint
- Microsoft SQL Serve -- Protezione per i Server SQL, incluso il database di Server Enterprise per BlackBerry.
- Microsoft IIS Server -- Protezione per Internet Information Systems.
- Il Microsoft Hyper-V -- Protezione per ambienti virtualizzati.
- Microsoft Dynamics CRM -- Protezione per i server Dynamics CRM.
- Database Oracle -- Protezione per i database Oracle.
- Server VMware vCenter -- Protezione per ambienti virtualizzati.
- Servizio di controllo di Arcserve RHA -- Protezione per questo componente di Arcserve RHA.
- HA per sistemi completi -- Trasferimento di un intero computer (fisico o virtuale) a un computer virtuale (Hyper-V, VMware ESX, and Citrix XEN Server).

Nota: È possibile proteggere i server BlackBerry Enterprise utilizzando Arcserve RHA per Microsoft SQL Server o file server, a seconda della configurazione in uso. Per ulteriori dettagli, si rimanda alla Guida operativa per BlackBerry Enterprise Server di Arcserve RHA.

Per un elenco aggiornato delle piattaforme e applicazioni supportate, consultare l'articolo *Supported Configurations* sul sito Arcserve.com.

Le proprietà configurate durante la creazione dello scenario variano a seconda dell'applicazione o del server database che si desidera proteggere. La *Guida per l'amministratore* illustra le singole proprietà. Per ulteriori istruzioni sulla creazione di scenari specifici, consultare la relativa *Guida operativa*

Concetti di Arcserve RHA

I seguenti concetti descrivono le modalità di protezione degli ambienti server da parte di Arcserve RHA.

Funzionamento della sincronizzazione (a pagina 18)

Funzionamento della replica (a pagina 21)

Funzionamento del recupero (a pagina 22)

Funzionamento del ripristino dei dati (a pagina 23)

Funzionamento della sospensione della replica (a pagina 23)

Funzionamento di High Availability (a pagina 24)

Funzionamento della sincronizzazione

La sincronizzazione dei file è il processo che rende il set di file da proteggere identico sui server master e di replica. Il passaggio iniziale di uno scenario di replica consiste di norma nella sincronizzazione del server master e del server di replica.

Importante: si consiglia di eseguire la sincronizzazione iniziale durante gli orari di minor traffico.

I file sparse vengono sincronizzati come tali se supportati dal volume sul server di replica. In caso contrario, gli attributi di tali file verranno persi durante i processi di replica o di sincronizzazione.

Metodi di sincronizzazione

Per sincronizzare correttamente il server master e di replica, è necessario eseguire innanzitutto un confronto tra le relative strutture file. Tale confronto consente di determinare quali contenuti (file e cartelle) sul server master sono mancanti oppure diversi rispetto a quelli sul server di replica. La sincronizzazione può essere avviata in due modi:

- Fare clic sul pulsante Sincronizza sulla barra degli strumenti della Gestione
- Fare clic sul pulsante Esegui sulla barra degli strumenti della Gestione

Selezionare una modalità di sincronizzazione, assegnando ad ognuna un algoritmo di confronto e un metodo di operazione differenti:

Sincronizzazione file

Nella sincronizzazione file, il server di replica invia la propria snapshot al server master, che la utilizza per gestire le informazioni e i contenuti per il confronto dei dati. Dopo aver eseguito il confronto, il modulo sul server master invia una sequenza di comandi al server di replica. Tali comandi:

- eliminano file presenti solo sulla destinazione
- elencano il contenuto dei file presenti solo sul server Master o dei file presenti sulla replica che differiscono dalla versione del Master

Questo metodo è più indicato per file server o server di applicazioni che presentano numerosi file di dimensioni relativamente ridotte.

Nota: durante l'esecuzione della sincronizzazione file, Arcserve RHA non aggiorna la percentuale di dati trasferiti fino al completamento del trasferimento dei file.

Sincronizzazione a blocchi

Nella Sincronizzazione a blocchi, il modulo esegue un confronto blocco per blocco dei file master e replica e copia solo i blocchi differenti. Se sono presenti differenze tra un file e l'altro, non viene trasferito l'intero file ma solo gli elementi differenti.

Questo metodo è ideale per applicazioni di database, quali Microsoft Exchange Server, Oracle e SQL Server, oppure per server applicazioni con file di dimensioni molto grandi.

Sincronizzazione non in linea (disponibile solamente dalla finestra di dialogo Esegui)

Nella sincronizzazione non in linea, i dati vengono copiati dal server master su una periferica esterna, e dalla periferica esterna al server di replica. Lo scenario di sistema completo supporta il metodo di sincronizzazione non in linea per gli scenari precedente. successivo e di ripristino BMR.

Questo metodo facilita il trasferimento di volumi di dati di grandi dimensioni evitando conseguenze derivanti da una larghezza di banda di rete insufficiente. Questa opzione è disponibile solamente durante l'esecuzione di uno scenario e non è applicabile a scenari con replica pianificata, o scenari con host master UNIX/Linux. Per ulteriori informazioni, consultare la sezione Funzionamento della sincronizzazione non in linea. (a pagina 133)

Sincronizzazione volume (disponibile soltanto per scenari di sistema completi)

Nella sincronizzazione del volume, il server Master copia il volume come intero invece di un file o un blocco. Tutti i volumi su un disco vengono sincronizzati a livello del volume. RHA esegue l'accesso al bitmap e copia soltanto i dati utilizzati. Ad esempio, quando il volume utilizzato corrisponde a 25 GB di un volume di 50 GB, verranno copiati soltanto i 25 GB utilizzati.

Nota: se la dimensione dei volumi master sono superiori a quelle della replica, RHA passa alla sincronizzazione dei blocchi.

Il confronto può essere configurato in modo da considerare solo la dimensione del file e la data di modifica, in modo da determinare se due file sono differenti oppure eseguire un controllo del contenuto effettivo dei dati. Il primo approccio (non valido nel caso di applicazioni di database), può accelerare in modo significativo il processo di confronto in uno scenario file server.

È possibile filtrare o ignorare la sincronizzazione.

Filtri di sincronizzazione

Prima di avviare la sincronizzazione, è possibile applicare un filtro al processo di sincronizzazione. Questo filtro, denominato **Ignora file della stessa dimensione/data,** viene visualizzato nella finestra di dialogo **Esegui** e può essere abilitato o disabilitato.

Il filtro **Ignora file della stessa dimensione/data** consente di confrontare i dati tra il server master e il server di replica, in modo da tenere conto solo della dimensione e della data di modifica dei file durante la determinazione delle differenze tra due file. Il filtro consente di non eseguire il confronto di file con lo stesso percorso, nome, dimensione e data di modifica, supponendo che tali file siano identici. Questo approccio non è valido nel caso di applicazioni di database, ma può essere un metodo efficiente per accelerare in modo significativo il processo di confronto in una soluzione file server e ridurre radicalmente la durata complessiva della sincronizzazione.

Importante: *NON* saltare la fase di sincronizzazione se non si è assolutamente sicuri che i file sui server master e di replica sono identici.

Sincronizzazione automatica

È possibile configurare il sistema in modo da eseguire una sincronizzazione automatica quando si verificano determinati eventi. La proprietà di Sincronizzazione automatica comporta la risincronizzazione automatica dei server master e replica se si verifica uno dei seguenti eventi:

- La replica viene riavviata.
- Il master viene riavviato.

Nota: se si verifica un overflow dello spool master a causa di un errore di rete, i server vengono risincronizzati automaticamente con il ripristino della connessione.

È possibile impostare la proprietà Sincronizzazione automatica nelle proprietà dello scenario relative al gruppo della replica.

Sincronizzazione e replica simultanee

Con la sincronizzazione e la replica simultanee è possibile sincronizzare i server mentre i file sono in uso o in fase di aggiornamento. Tutte le modifiche applicate durante l'esecuzione della sincronizzazione iniziale vengono replicate senza la necessità di un 'intervento amministrativo.

Segnalazione delle differenze di sincronizzazione

È possibile verificare le eventuali differenze tra i set di dati sui server master e di replica senza eseguire la risincronizzazione tramite l'opzione Rapporto delle differenze (a pagina 169).

Funzionamento della replica

Il meccanismo di replica mantiene copie identiche dei file e dei database sul server master e di replica. La replica viene eseguita tramite acquisizione in tempo reale di modifiche a livello di byte apportate ai file sul server master, utilizzando un driver di filtro del file system. Le modifiche acquisite vengono trasmesse in modo asincrono ai server di replica mediante il modulo. Il processo di replica non interferisce con le operazioni di scrittura.

Per adeguare la replica in tempo reale a tutti i tipi di file, sono supportate le seguenti modalità di replica:

- **Modalità in linea** - Replica le modifiche dei file acquisite, anche se i file sono sempre aperti (come nel caso della maggior parte dei database e dei server di posta elettronica). Questa modalità mantiene l'ordine delle operazioni del file system. In questa modalità, il modulo registra tutte le operazioni di I/O correlate alle directory principali nei file diario. I file diario vengono poi inviati ai server di replica, dove le operazioni che erano state registrate nel diario vengono riprodotte sui file replicati.
- **Modalità di pianificazione** - La sincronizzazione dei server ha luogo a orari prestabiliti. In questa modalità non viene eseguita la replica in linea; tuttavia, le modifiche in linea apportate durante la sincronizzazione verranno replicate. (La replica pianificata non può essere eseguita con la sincronizzazione non in linea.)

È possibile, inoltre, valutare accuratamente l'utilizzo della larghezza di banda e il benchmarking del rapporto di compressione necessario per la replica., senza effettivamente replicare i dati. Quando si seleziona la modalità di valutazione, non viene eseguita una replica, ma verranno raccolti dati statistici. Al completamento del processo di valutazione verrà fornito un rapporto.

I file frammentati sono ora supportati. I file frammentati sono file di grandi dimensioni che contengono un numero elevato di zero. Quando i file system NTFS individuano esecuzioni di dati zero di grandi dimensioni, gli zero no vengono scritti esplicitamente sul disco. Il file system, invece, conserva una traccia della posizione delle esecuzioni dei dati zero. Sebbene la dimensione del file riportata sia la stessa, lo spazio utilizzato sul disco è inferiore. Arcserve RHA assicura la coerenza di contenuto nei file frammentati. Non è possibile replicare i file frammentati su un server di replica non in grado di supportare tali file, come ad esempio una replica di FAT32.

Le operazioni relative ai file frammentati sono trasparenti e gestite internamente.

Funzionamento del recupero

Quando, per un qualsiasi motivo, si verifica la perdita o il danneggiamento dei dati del server master, è possibile recuperare tali dati da uno dei server di replica facenti parte dello scenario. L'opzione Ripristino dei dati attiva un processo di sincronizzazione in direzione inversa, dal server di replica al server master.

All'avvio del ripristino, la Gestione crea una struttura temporanea formata da un unico ramo. In questa struttura, la replica diventa la fonte dei dati e il server master originario diventa la destinazione (cioè, il server di replica di chiusura). Al termine del processo di sincronizzazione, la Gestione torna allo scenario di replica originario e continua il suo normale funzionamento.

Importante: tutte le attività di file system devono essere interrotte sull'host master fino al completamento del processo di ripristino.

Funzionamento del ripristino dei dati

Il ripristino dei dati è una tecnologia che consente di riparare un file danneggiato tornando indietro nel tempo, proprio come se si riavvolgesse un nastro. Dato che la replica aggiorna continuamente l'origine dati su un altro computer, su un server di replica sono sempre presenti gli stessi dati del server master. Nel caso di danneggiamento dei dati, il recupero dei file più aggiornati dal server di replica non risolverà il problema, dato che ci sono forti probabilità che anche i dati sul server di replica siano danneggiati.

Il ripristino dei dati può essere comparato alla funzione Annulla presente in diverse applicazioni di produttività che consente di annullare le azioni dell'utente, riportando il file allo stato precedente alle modifica. Il ripristino dei dati si basa su diari di ripristino in cui sono memorizzate le informazioni sulle operazioni di I/O che risultano nei file modificati. Mediante l'utilizzo del diario di ripristino è possibile *annullare* le operazioni I/O. In questo modo, il file viene ripristinato a uno stato precedente nel tempo, quindi a uno stato valido e non danneggiato.

Funzionamento della sospensione della replica

A volte può essere necessario sospendere gli aggiornamenti sul computer di un server di replica allo scopo di eseguire la manutenzione del sistema o qualche altra forma di elaborazione che non modifica i dati ivi replicati. Si consiglia di non interrompere la replica, altrimenti in seguito sarà necessario eseguire una risincronizzazione.

La funzione di sospensione della replica consente di risolvere questo problema. La replica può essere sospesa manualmente o su base pianificata. Durante il periodo di sospensione, tutte le modifiche vengono inserite nello spool sul server master o sul server di replica situato a monte del server di replica sospeso. In altri termini, la registrazione delle modifiche continuerà a essere eseguita per l'aggiornamento del server di replica sospeso, ma il trasferimento effettivo non verrà eseguito fino alla ripresa della replica. Dopo la ripresa della replica, le modifiche accumulate vengono trasferite e applicate senza dover eseguire una risincronizzazione dei dati.

Per procedere alla sospensione della replica, scegliere Strumenti e l'opzione di sospensione della replica dal menu Gestione.

Funzionamento di High Availability

Arcserve RHA monitora tutti gli eventi di importanza critica, incluso il malfunzionamento del server globale e tutti gli errori del servizio di database Arcserve RHA può essere configurato per invertire automaticamente i ruoli del server (failover) oppure per scambiarli manualmente (avanzamento) quando viene rilevato un evento critico. Ciò significa che il server di replica diventa attivo quando il server master è fermo.

Nota: le impostazioni di failover automatico e di avanzamento manuale vengono configurate durante la creazione degli scenari High Availability. Ad ogni modo, tali impostazioni possono essere configurate anche dalla scheda di gestione proprietà di Arcserve RHA, espandendo il gruppo di proprietà delle impostazioni di avanzamento.

Se il server master non è disponibile, le sue attività passeranno automaticamente a un sito remoto (replica). Il failover, che è trasparente all'utente, include l'avvio immediato di un database in stand-by sincronizzato. Tutti gli utenti vengono ridiretti a tale database in tempo rapido. Tutto ciò può essere eseguito senza la necessità di riconfigurare i clienti o la rete.

Il reindirizzamento può essere basato sui metodi seguenti:

- IP di spostamento (se il sito in stand-by è implementato all'interno dello stesso segmento di rete)
- Reindirizza DNS: può essere usato su una rete locale o quando il sito in stand-by remoto si trova su una diversa rete IP (avanzamento tra più reti)
- Sostituzione del nome host/nome NetBIOS del server

Nota: è anche possibile applicare script definiti dall'utente che integrino o sostituiscano i metodi di reindirizzamento incorporati. Gli script di identificazione della direzione del traffico di rete sono richiesti per supportare i metodi di reindirizzamento personalizzati. Gli script personalizzati o file di batch vengono utilizzati per identificare il server attivo. Questo script determina se lo scenario successivo o precedente verrà eseguito all'avvio dello scenario. Lo script viene eseguito sia sul server master sia sul server di replica: quello tra i due che restituisce un valore pari a zero è il server attivo. Se entrambi restituiscono zero, verrà segnalato un conflitto.

La selezione del metodo di reindirizzamento si basa sui requisiti delle applicazioni da proteggere. È possibile che alcuni metodi non siano compatibili con un determinato scenario. Per ulteriori informazioni, consultare la guida operativa specifica dell'applicazione.

Funzionamento di Assured Recovery per file server

Durante la creazione di scenari file server, è possibile scegliere l'opzione Verifica integrità per Assured Recovery (AR) dalla finestra di dialogo Selezionare server e tipo di prodotto. È possibile pianificare una verifica. Fare doppio clic sul valore relativo a Pianifica per aprire la schermata Ore Assured recovery.

Per impostazione predefinita, Assured Recovery per file server acquisisce snapshot VSS sul server di replica durante il test. Tali snapshot utilizzano spazio sul volume della replica. Per impostazione predefinita, le snapshot VSS sono disattivate per evitare problemi di spazio sul disco.

Nota: non esiste alcuna applicazione in scenari file server, per cui la verifica Assured Recovery richiede script personalizzati.

Limitazioni

È consentita esclusivamente la replica asincrona e unidirezionale e il database non deve essere in linea. La replica bidirezionale non è supportata. Tuttavia, è supportata la replica incrociata con diversi set di dati. Un server su cui è in esecuzione Arcserve RHA può fungere da server master e di replica per un numero illimitato di scenari a patto che ciascun set di dati disponga di un unico server master, ovvero di una replica unidirezionale.

Componenti di Replication e High Availability

Arcserve RHA è costituito dai seguenti componenti:

- Servizio di controllo (a pagina 25)
- Modulo (a pagina 26)
- Centro di gestione (a pagina 27) -- Consta a sua volta di tre componenti: Pagina con informazioni introduttive, Gestione e Report Center.
- PowerShell (a pagina 28)
- Arcserve RHA per il cluster di failover Microsoft (a pagina 28)

Servizio di controllo

Il Servizio di controllo serve come single-point-di-controllo nelle operazioni di replica o di High Availability. Contiene l'intero set di dati degli scenari esistenti. Il Servizio di controllo comunica con i moduli e con le Gestioni. Il Servizio di controllo consente di gestire tutte le attività associate agli scenari, quali creazione, configurazione, monitoraggio ed esecuzione degli scenari stessi.

Le richieste provenienti dalla/e Gestione/i vengono ricevute, elaborate, convertite in particolari comandi e inviate ai Moduli. Successivamente, dopo aver ricevuto dati ed eventi aggiornati dai Moduli, alla Gestione vengono restituite informazioni e statistiche sullo stato dello scenario.

Il Servizio di controllo serve anche per l'autenticazione e l'autorizzazione degli utenti, oltre a poter fungere da punto centrale per la gestione e l'archiviazione dei rapporti. Le informazioni e le statistiche raccolte dal Servizio di controllo possono essere presentate all'utente attraverso la Pagina con informazioni introduttive, la Gestione, il Report Center e PowerShell.

Tutti i file dello scenario vengono conservati nel server su cui è in esecuzione il Servizio di controllo. Anche se il Servizio di controllo non è attivo, il funzionamento dello scenario non ne risente. Tuttavia, per poter ricevere informazioni sullo stato dello scenario, il Servizio di controllo deve essere attivo. Per ottenere migliori risultati, installare il Servizio di controllo su un host standalone. Se questo non è possibile, installare il Servizio di controllo sul server master o sul server di replica. Se il server risulta inattivo, la connessione con il Servizio di controllo non è più disponibile e gli scenari risulteranno non gestibili.

È possibile proteggere il Servizio di controllo di Arcserve RHA in scenari separati. Per ulteriori informazioni, consultare Protezione del Servizio di controllo (a pagina 295) nella *Guida per l'amministratore di Arcserve RHA*.

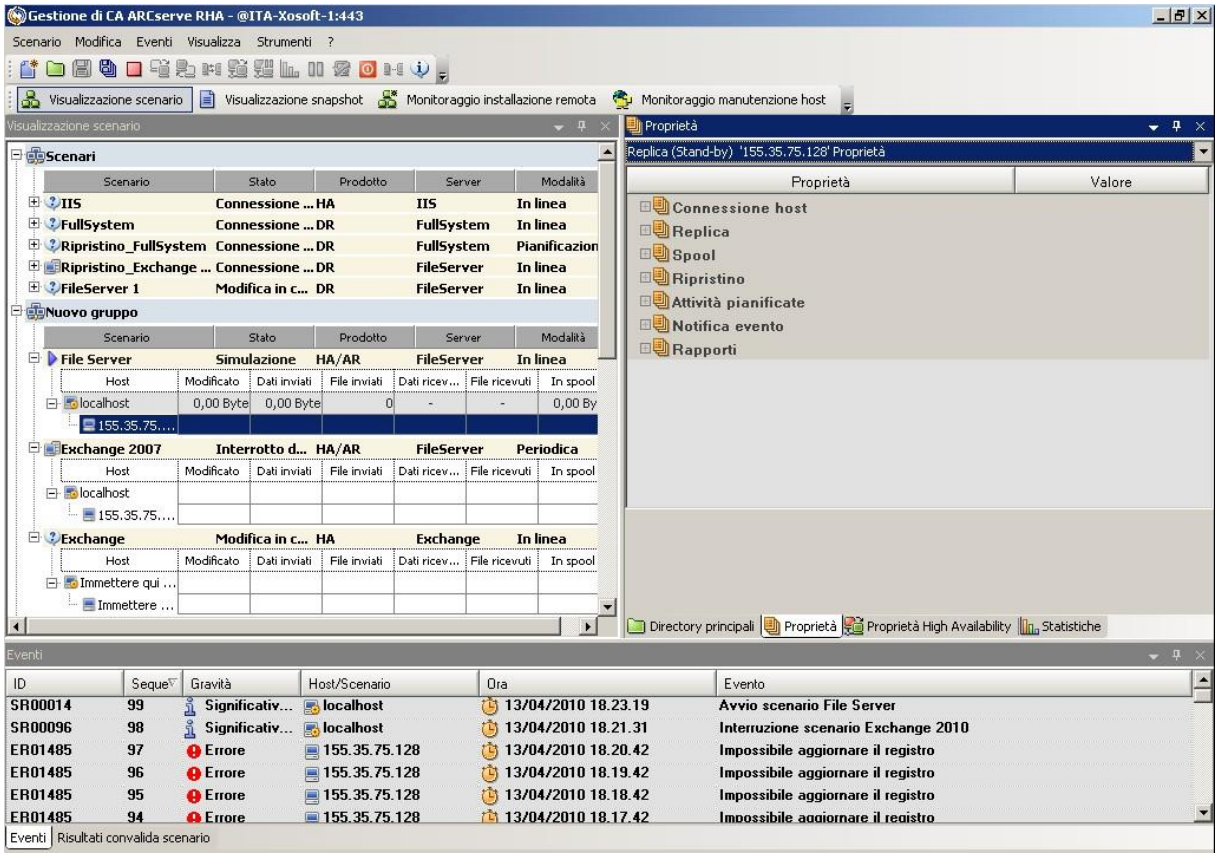
Modulo

Il modulo è un servizio che deve essere in esecuzione prima di procedere all'avvio di uno scenario. È installato su tutti i server che rientrano in un determinato scenario, ossia l'host master (origine) e quello di replica (destinazione). Nel modulo vengono supportate le funzionalità del master e della replica per gli scenari Replication e High Availability. Il modulo può rientrare in più scenari, assumendo in ciascuno una funzione diversa. È possibile installare i moduli localmente su un host alla volta oppure su più host contemporaneamente utilizzando l'installazione remota. Se necessario, i moduli possono essere installati durante la creazione dello scenario.

Centro di gestione

Il Centro di gestione consta di tre componenti, nessuno dei quali richiede un'installazione manuale:

- **Pagina con informazioni introduttive** - Una panoramica statistica dello stato dello scenario Replication e High Availability.
- **Gestione** - Un'interfaccia utente che consente di creare, configurare, gestire e monitorare gli scenari. Si tratta di un'interfaccia utente che viene attivata dalla Pagina con informazioni introduttive facendo clic sul collegamento Gestione scenario.


Gestione di CA ARCserve RHA - @ITA-Xosoft-1:443
Scenario Modifica Eventi Visualizza Strumenti ?
Visualizzazione scenario
Visualizzazione snapshot
Monitoraggio installazione remota
Monitoraggio manutenzione host
Visualizzazione scenario
Scenari
Scenario Stato Prodotto Server Modalità
IIS Connessione ... HA IIS In linea
FullSystem Connessione ... DR FullSystem In linea
Ripristino_FullSystem Connessione ... DR FullSystem Pianificazion
Ripristino_Exchange ... Connessione ... DR FileServer In linea
FileServer 1 Modifica in c... DR FileServer In linea
Nuovo gruppo
File Server Simulazione HA/AR FileServer In linea
Exchange 2007 Interrotto d... HA/AR FileServer Periodica
Exchange Modifica in c... HA Exchange In linea
Proprietà
Replica (Stand-by) '155.35.75.128' Proprietà
Proprietà Valore
Connessione host
Replica
Spool
Ripristino
Attività pianificate
Notifica evento
Rapporti
Directory principali
Proprietà
Proprietà High Availability
Statistiche
Eventi
ID Seque Gravità Host/Scenario Ora Evento
SR00014 99 Significativ... localhost 13/04/2010 18.23.19 Avvio scenario File Server
SR00096 98 Significativ... localhost 13/04/2010 18.21.31 Interruzione scenario Exchange 2010
ER01485 97 Errore 155.35.75.128 13/04/2010 18.20.42 Impossibile aggiornare il registro
ER01485 96 Errore 155.35.75.128 13/04/2010 18.19.42 Impossibile aggiornare il registro
ER01485 95 Errore 155.35.75.128 13/04/2010 18.18.42 Impossibile aggiornare il registro
ER01485 94 Errore 155.35.75.128 13/04/2010 18.17.42 Impossibile aggiornare il registro
Eventi
Risultati convalida scenario

- **Report Center** - Un'interfaccia utente che consente di raccogliere tutti i rapporti esistenti, con informazioni sui report disponibili per scenario. È possibile stabilire la destinazione di archiviazione dei rapporti e per quanto tempo potranno essere visualizzati e mantenuti nel Report Center.

PowerShell

PowerShell costituisce un'alternativa alla gestione del processo di replica mediante l'interfaccia grafica utente di gestione. Oltre ad ampliare e semplificare le funzionalità CLI presenti nelle versioni precedenti, supporta operazioni di replica e HA.

PowerShell è un ambiente shell e di script a riga di comando che consente di configurare uno scenario di replica e di controllare e monitorare il processo di replica. Tutti gli scenari gestiti da PowerShell hanno esattamente lo stesso aspetto e funzionamento di quelli di competenza della Gestione e vengono salvati automaticamente nello stesso percorso predefinito: INSTALL_DIR/ws_scenarios.

PowerShell si basa sulla shell standard Windows PowerShell™, dotata di un'ampia serie di comandi incorporati all'interno di un'interfaccia omogenea. Il componente PowerShell aggiunge diversi comandi per lo scenario, denominati snap-in, che facilitano la gestione dello scenario.

Arcserve RHA per il cluster di failover Microsoft

Arcserve RHA per il cluster di failover Microsoft include un plug-in della risorsa disco virtuale e un'interfaccia semplificata installata su tutti i nodi del cluster.

Sebbene High Availability non sia integrato in ambienti cluster di Microsoft, l'archiviazione condivisa può corrispondere a un singolo punto di errore. Arcserve RHA protegge l'archiviazione cluster e consente di replicare i dati su una risorsa disco locale o esterna.

Modalità di distribuzione di Arcserve RHA

La distribuzione dei componenti di Arcserve RHA dipende dalla dimensione della rete IT aziendale, dalla replica e dalle esigenze HA. Ad ogni modo, esistono delle linee guida da seguire nella progettazione del proprio ambiente di utilizzo e nella distribuzione dei diversi componenti su piattaforme Windows. Per informazioni riguardo la distribuzione efficiente, consultare la *Guida all'installazione* di *Arcserve RHA*.

In generale, si procede all'installazione del modulo su due server - un server master un server replica. Il Servizio di controllo dovrebbe essere installato su un server standalone per garantirne la protezione nello scenario. Per ulteriori informazioni, consultare la sezione Protezione del Servizio di controllo (a pagina 295).

Capitolo 2: Esplorazione della Gestione

Questa sezione descrive la Gestione e i relativi componenti e funzionalità. In essa sono contenute istruzioni su come accedere al Centro di gestione e alla Gestione e si procede alla descrizione della struttura, dei menu, dei pulsanti e delle funzioni disponibili nella finestra principale della Gestione.

Questa sezione contiene i seguenti argomenti:

Accesso al Centro di gestione (a pagina 30)
Collegamenti per l'accesso al supporto tecnico e alla community (a pagina 32)
Esplorazione della schermata Gestione di Arcserve RHA (a pagina 34)
Visualizzazione e organizzazione della schermata Gestione (a pagina 37)
Barre degli strumenti (a pagina 41)
Registrazione licenze di Arcserve RHA (a pagina 45)

Accesso al Centro di gestione

Il Centro di gestione e la Gestione non richiedono l'installazione preventiva di componenti o applicazioni. Si tratta di una procedura di installazione con un clic che può essere eseguita da qualsiasi workstation dotata di connessione di rete e browser. Per effettuare l'accesso, sono necessari i seguenti dati.

- Nome host/Indirizzo IP e numero di porta del server su cui è installato il Servizio di controllo.
- Nome utente, password e dominio dell'host.

Per aprire la Gestione:

1. Aprire Internet Explorer. Nella casella **Indirizzo**, immettere il nome host/l'indirizzo IP e il numero di porta del Servizio di controllo come segue:

   `http://host_name:port_no/start_page.aspx`

   Viene visualizzata la finestra di dialogo **Accesso**.

   Tenere presenti le seguenti considerazioni:

   - Se il Centro di gestione viene aperto dal computer su cui è installato il Servizio di controllo, utilizzare i parametri predefiniti:

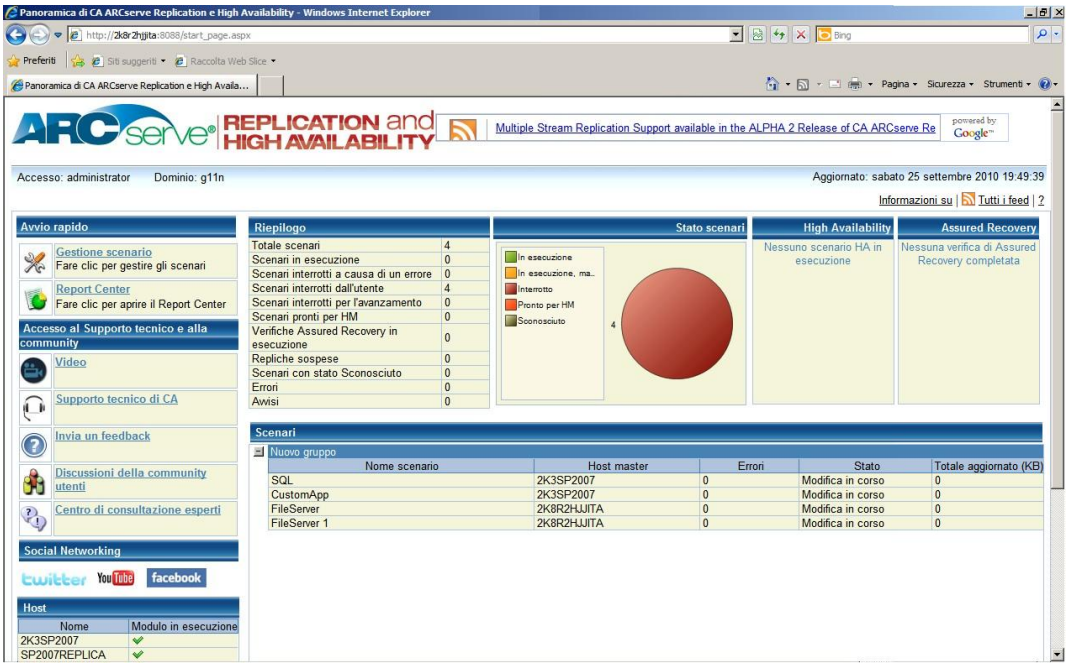
     `http://localhost:8088/start_page.aspx`

   - Se è stata selezionata l'opzione **Configurazione SSL** durante l'installazione del Servizio di controllo**,** quando si procede all'apertura della Pagina con informazioni introduttive è necessario utilizzare il nome host del computer del Servizio di controllo (anziché l'indirizzo IP corrispondente). Immettere il nome host e il numero di porta del Servizio di controllo come segue:
     `https://nome_host:numero_porta/pagina_avvio.aspx`

2. Immettere nome utente, password e dominio, quindi fare clic su **Accedi**.

   Importante: per accedere al Centro di gestione, è necessario essere membri del gruppo Administrators nel computer locale in cui è installato il Servizio di controllo.

   Viene visualizzata la **Pagina con informazioni introduttive**.



3. Nella barra degli strumenti **Avvio rapido** a sinistra, fare clic sull'opzione **Gestione scenario**.

   Viene visualizzata una barra di avanzamento che indica che il componente Gestione è attualmente installato nel computer locale.

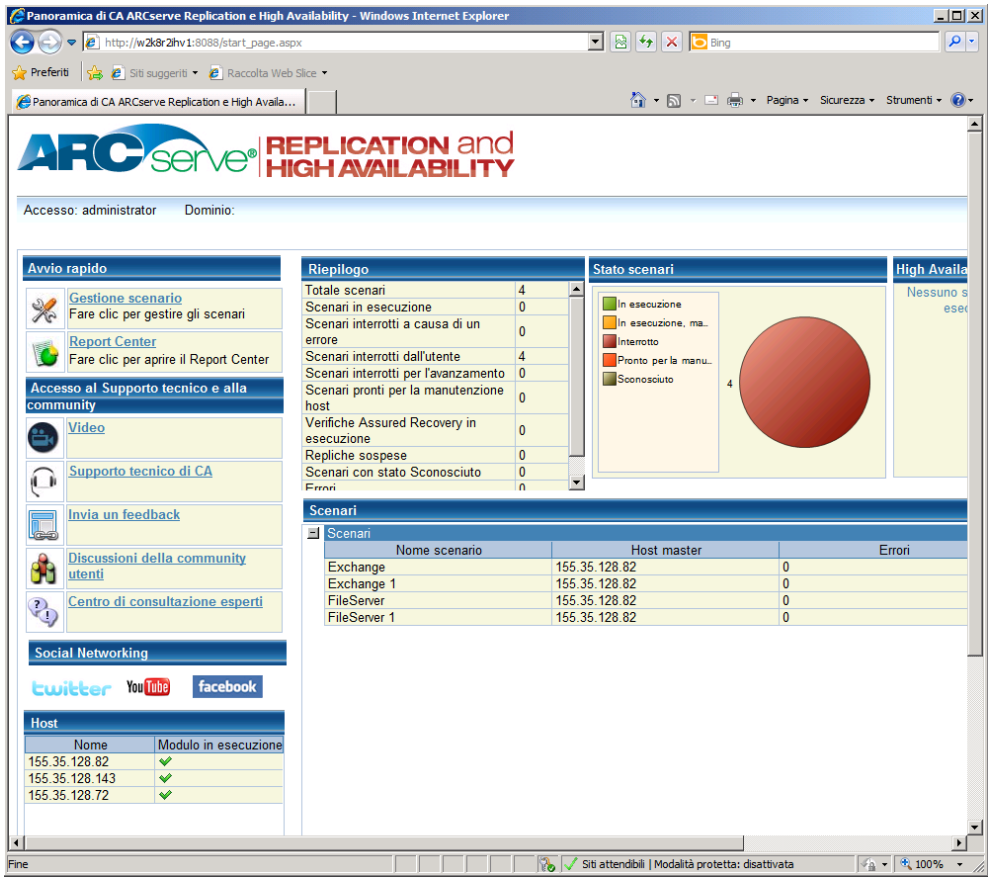
4. Al termine dell'installazione, il componente viene visualizzato:

   Importante. La Gestione consente l'accesso simultaneo di più amministratori. Gli amministratori possono apportare modifiche in qualsiasi momento, a seconda dei privilegi di cui dispongono. L'ultimo aggiornamento verrà considerato come lo stato più recente dello scenario. Di conseguenza, quando più amministratori lavorano tutti allo stesso tempo sulla Gestione, è necessario considerare che potrebbero verificarsi sovrascritture involontarie delle modifiche apportate da parte di altri amministratori. Si consiglia di adottare misure interne idonee al fine di prevenire tale evenienza.

Collegamenti per l'accesso al supporto tecnico e alla community

La schermata delle informazioni introduttive è stata ridisegnata per incorporare le più recenti tecnologie di Internet. Nella parte superiore della schermata, sarà possibile trovare un flusso di feed RSS con i titoli degli articoli relativi ai prodotti. Fare clic su un titolo per visualizzare l'articolo completo pubblicato nel Centro di consultazione esperti.

La sezione di accesso al supporto tecnico e alla community della pagina principale di Arcserve RHA fornisce collegamenti ai siti di supporto di vari prodotti.



Video

Fare clic qui per accedere ai video esplicativi di Arcserve RHA relativi alle procedure di base. I video possono anche essere visualizzati direttamente da YouTube. (Fare clic sul collegamento di YouTube nel pannello Social Networking.)

Supporto tecnico di Arcserve

Fare clic qui per accedere al sito del supporto tecnico, dal quale procedere alla risoluzione problemi e visualizzare importanti informazioni sul prodotto.

Invia un feedback

Soddisfa le tue curiosità e condividi le tue idee sulle nuove funzionalità del prodotto attraverso il nostro partner *GetSatisfaction*. Tutte le informazioni vengono inoltrate direttamente al team di sviluppo del prodotto.

Discussione della community di utenti

Entra a far parte della community utenti di Arcserve RHA Fare clic qui per condividere suggerimenti e best practice o per fare una domanda.

Centro di consultazione esperti

Abbonati al newsfeed per essere sempre al corrente delle ultime novità di prodotto e per ricevere informazioni o collegamenti relativi a Arcserve RHA.

Social networking

Potrai restare al corrente delle novità di prodotto anche su Twitter o Facebook! Per accedere al video, fare clic sul collegamento YouTube.

Per abbonarsi ad alcuni siti o a tutti, fare clic su Tutti i feed (nell'angolo superiore destro della pagina). Qualunque aggiornamento del sito verrà notificato agli utenti.

È possibile abilitare o disabilitare i feed (disabilitati per impostazione predefinita) e i collegamenti di social networking (abilitati per impostazione predefinita) in base alle proprie esigenze. Per abilitare tali impostazioni, modificare il file di configurazione come indicato di seguito:

1. Aprire il file web.config da [Install dir]/ws_root.
2. Individuare e impostare le seguenti impostazioni:

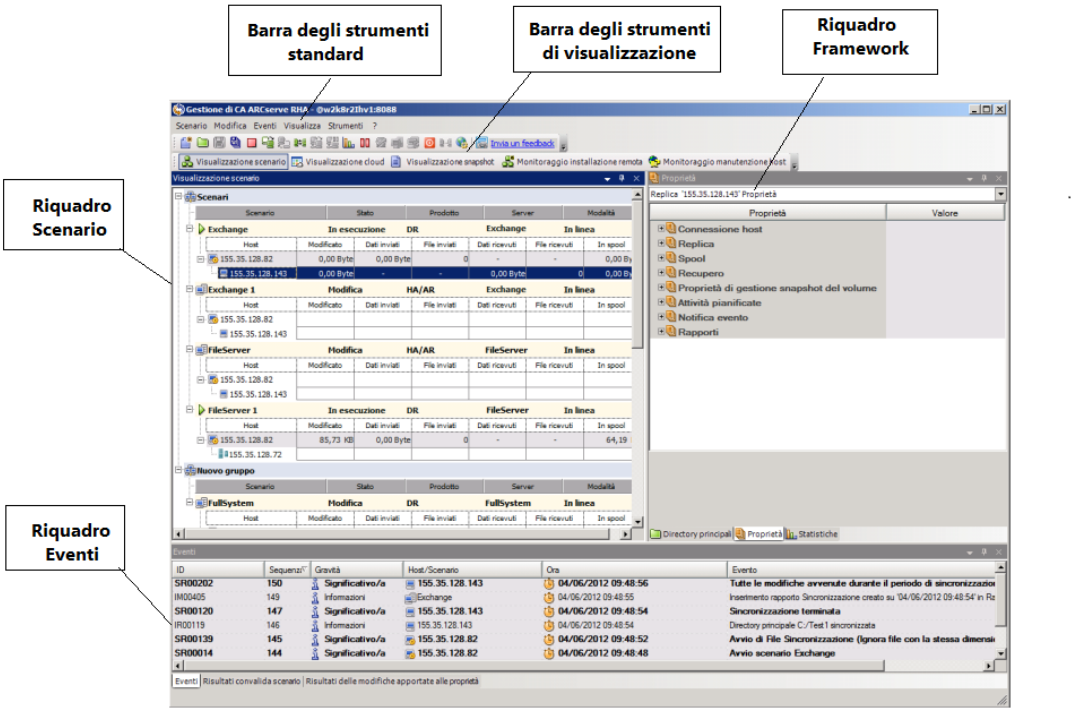
```
<appSettings>
    <add key="SocialNetwork_Visible" value="true" />
    <add key="GoogleFeed_Visible" value="false" />
</appSettings>
```

3. Salvare il file web.config.

Esplorazione della schermata Gestione di Arcserve RHA

Dopo aver eseguito l'accesso all'applicazione, viene visualizzata la schermata della Gestione, che consente di accedere a tutti i menu, alle funzioni della barra degli strumenti e ai riquadri di gestione.

A meno che esista già uno scenario, la maggior parte delle aree dell'utente è vuota. Gli scenari attivi esistenti vengono mostrati sul lato sinistro della schermata Gestione.

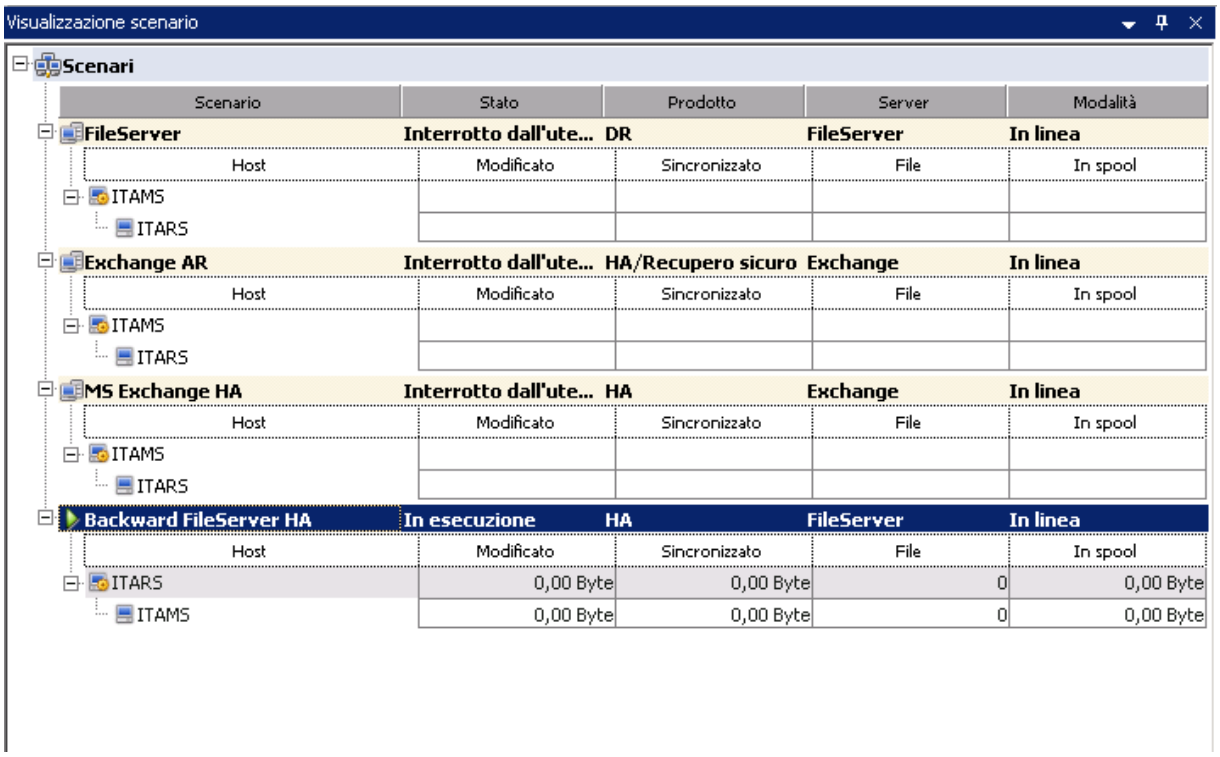


Nota: alcuni riquadri e alcune opzioni possono sono disponibili e attivati solo se si dispone della licenza appropriata per il prodotto.

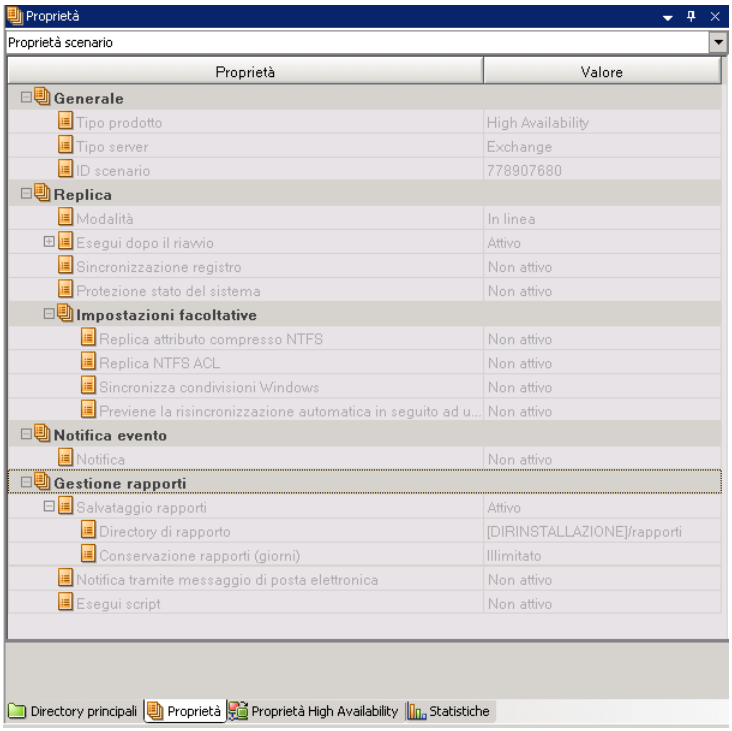
Riquadri della schermata Gestione

La schermata Gestione è suddivisa in diverse aree:

- Il nome dell'applicazione e i dettagli di connessione del Servizio di controllo vengono visualizzati nell'angolo in alto a sinistra della barra del titolo; al di sotto di essa, vengono visualizzate la barra dei menu, la barra degli strumenti standard e la barra degli strumenti di visualizzazione.
- Il riquadro Scenario viene visualizzato a sinistra. In questo riquadro vengono visualizzati gli scenari esistenti, incluse le strutture di replica.



- Il riquadro Struttura viene visualizzato a destra. In questo riquadro, vengono visualizzati gli elenchi delle proprietà configurabili: Scenario, Master, Replica, HA e Modello. L'elenco visualizzato dipende dall'elemento selezionato nel riquadro Scenario oppure dall'elemento prescelto nell'elenco a discesa del riquadro. Il riquadro Struttura contiene inoltre due, tre o quattro schede, a seconda della soluzione selezionata e dello stato dello scenario. Tali schede includono:
  - Directory principali
  - Proprietà
  - Proprietà High Availability
  - Statistiche



  Le proprietà visualizzate in ogni scheda sono descritte in modo più dettagliato nella sezione Impostazione proprietà Scenario (a pagina 201).

- Il riquadro Eventi è visualizzato sotto alla linea di divisione della schermata.

Nota: dal momento che è possibile spostare e ridimensionare i riquadri, la loro posizione effettiva può variare. Inoltre, in base alle selezioni nel menu Visualizza, è possibile nascondere i riquadri, incluso la barra degli strumenti e la barra di stato.

Visualizzazione e organizzazione della schermata Gestione

Arcserve RHA consente di visualizzare in diversi modi il proprio lavoro, a seconda dell'attività da svolgere. È possibile organizzare la propria area di lavoro in funzione delle esigenze correnti.

Nota: l'ultima impostazione di visualizzazione utilizzata verrà salvata per la sessione successiva.

Di seguito vengono descritti diversi metodi per la visualizzazione della schermata Gestione:

- Opzioni di visualizzazione (a pagina 37)
- Personalizzazione della visualizzazione scenario (a pagina 37)
- Riorganizzazione dei riquadri (a pagina 38)

Opzioni di visualizzazione

Il menu **Visualizza** contiene tutte le viste esistenti. La selezione di un'opzione di visualizzazione dal menu consentirà di aprire o chiudere il riquadro indicato.

Per reimpostare il layout della Gestione

1. Dal menu **Visualizza**, selezionare l'opzione Ripristina.

   Verranno ripristinate le impostazioni di visualizzazione originali.

Personalizzazione della visualizzazione scenario

Il riquadro Scenario mostra lo stato corrente per tutti gli scenari in un solo riquadro, consentendo all'utente di monitorare più scenari per volta. È possibile personalizzare la modalità di visualizzazione delle colonne informative dello scenario.

Per personalizzare la visualizzazione dello scenario, procedere come segue:

1. Dal menu Visualizza, scegliere l'opzione Personalizza visualizzazione scenario.

   Viene visualizzata la finestra di dialogo Personalizza visualizzazione scenario.

2. Selezionare i campi che si desidera visualizzare nel riquadro Scenario e fare clic su OK.

   Nota: il campo Avviato da indica l'utente che ha avviato l'esecuzione dello scenario.

   I campi selezionati dall'utente vengono visualizzati come colonne nel riquadro Scenario.

Riorganizzazione dei riquadri

È possibile ancorare, sovrapporre, nascondere, mostrare e rendere mobili i riquadri della Gestione in base alle proprie esigenze.

Ancorare un riquadro (a pagina 39)

Sovrapporre riquadri (a pagina 40)

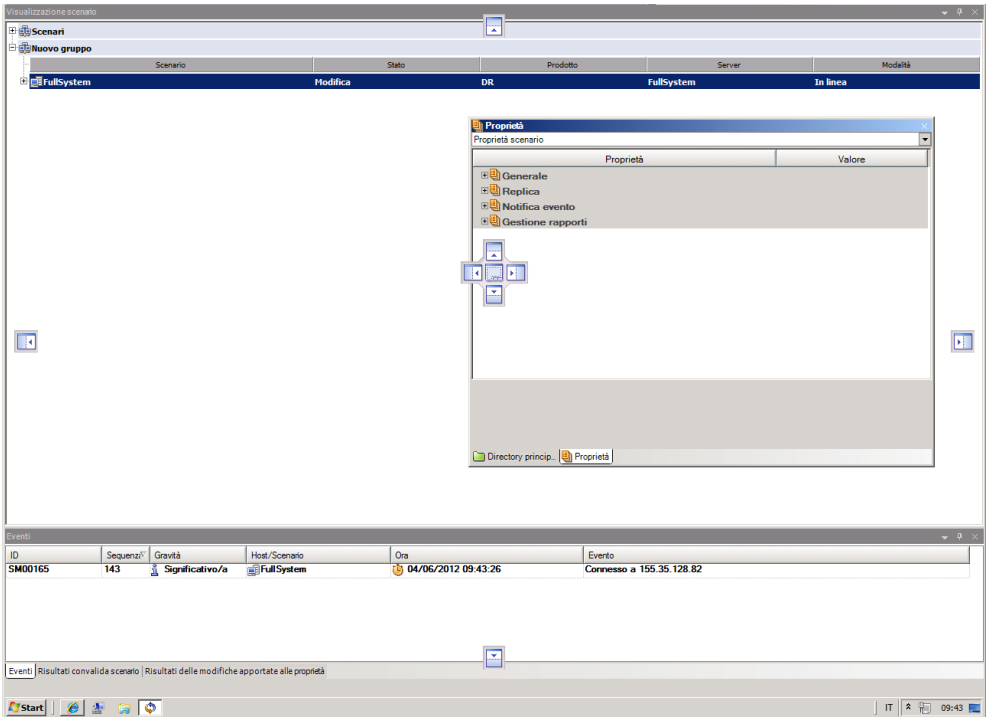
Nascondere riquadri (a pagina 41)

Ancorare un riquadro

Lo strumento di ancoraggio del riquadro, o guida a forma di rombo, è una funzionalità incorporata che viene visualizzata automaticamente quando si procede allo spostamento di un riquadro.

Per ancorare un riquadro, procedere come segue:

1. Dalla schermata della Gestione, fare clic sulla barra del titolo di un riquadro e trascinarla. Viene visualizzato lo strumento di ancoraggio riquadro.



2. Spostare il puntatore sopra a parte corrispondente allo strumento di ancoraggio del riquadro. È possibile utilizzare anche ai margini della finestra.
3. Rilasciare il pulsante del mouse una volta collocato il riquadro nella posizione desiderata.

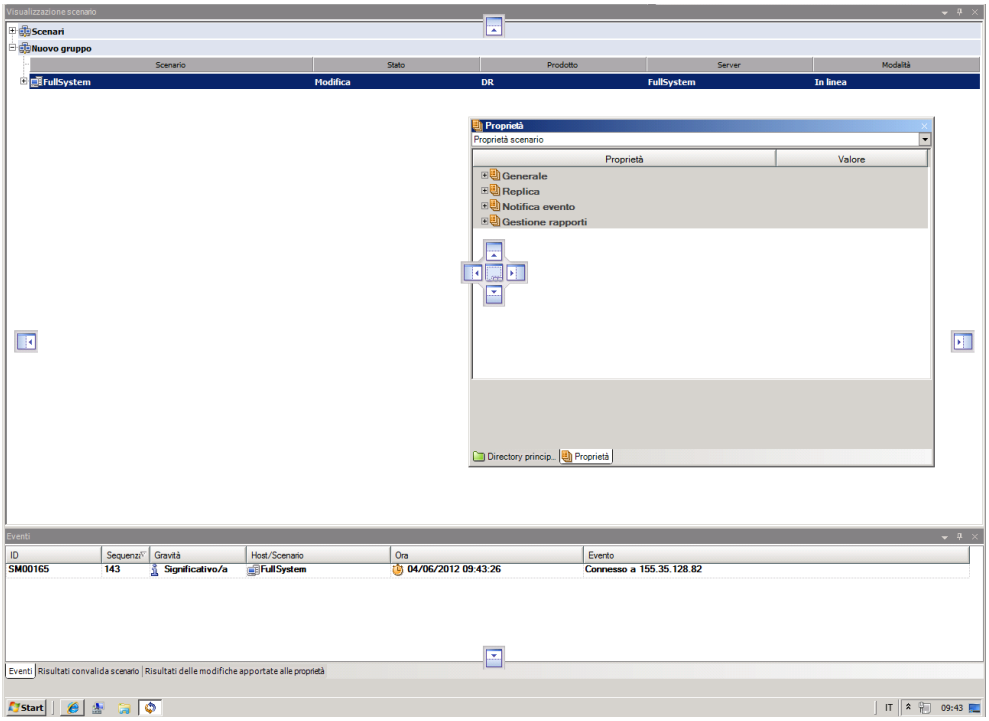
   Il riquadro viene ancorato nella nuova.posizione all'interno della schermata.

Sovrapporre riquadri

Sovrapponendo i riquadri uno sull'altro, ciascuno di essi verrà visualizzato come scheda nella schermata della Gestione.

Per sovrapporre i riquadri:

1. Dalla schermata della Gestione, fare clic sulla barra del titolo di un riquadro e trascinarla. Viene visualizzato lo strumento di ancoraggio riquadro.



2. Quando il riquadro che si sta trascinando avrà raggiunto un riquadro ancorato al quale si desidera sovrapporlo, spostare il puntatore al centro della guida a forma di rombo.
3. Rilasciare il pulsante del mouse.

   Il riquadro è ora accessibile facendo clic sulla relativa scheda.

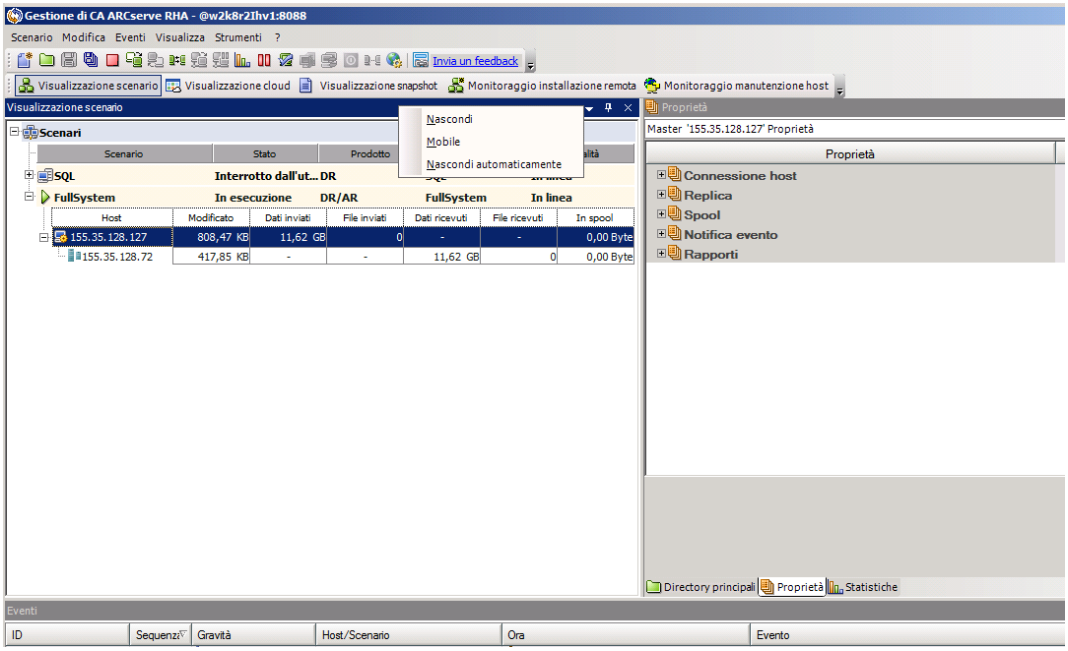
Nascondere riquadri

È possibile nascondere completamente un riquadro oppure nasconderlo solo quando si sta lavorando su un altro. Per tornare al riquadro nascosto, fare clic sulla scheda corrispondente.

Ripristinare i riquadri nascosti facendo clic sulle opzioni di menu Visualizza e quindi Ripristina.

Per nascondere un riquadro, procedere come segue:

1. Dalla schermata della Gestione, fare clic con il tasto destro del mouse sulla barra del titolo del riquadro. Viene visualizzato un menu di scelta di rapida.



2. Se si desidera nascondere completamente il riquadro, fare clic su Nascondi. Se si desidera nascondere il riquadro solo mentre si lavora su altri riquadri, fare clic su Nascondi automaticamente. Per tornare al riquadro di nascosto, fare clic sulla scheda corrispondente.

Barre degli strumenti

Arcserve RHA fornisce due barre degli strumenti per facilitare il lavoro dell'utente: la barra degli strumenti standard (a pagina 42) e la barra degli strumenti di visualizzazione (a pagina 45).

Barra degli strumenti standard

I pulsanti della barra degli strumenti standard consentono un accesso rapido alle funzioni più utilizzate della Gestione. Nell'elenco seguente viene riportata una breve descrizione di ciascuna opzione della barra degli strumenti.

Nuovo

Consente di creare un nuovo scenario utilizzando la creazione guidata. Per ulteriori informazioni, consultare la sezione Creazione di un nuovo scenario.

Gruppo

Consente di creare un nuovo gruppo di scenari. Per ulteriori informazioni, consultare la sezione Creazione di un gruppo di scenari (a pagina 74).

Salva

Consente di salvare uno scenario selezionato. Per ulteriori informazioni, consultare la sezione Salvataggio degli scenari (a pagina 195).

Salva tutto

Consente di salvare simultaneamente tutti gli scenari esistenti. Per ulteriori informazioni, consultare la sezione Salvataggio degli scenari (a pagina 195).

Esegui

Consente di eseguire lo scenario selezionato per avviare il processo di replica. Per ulteriori informazioni, consultare la sezione Avvio della replica (a pagina 127).

Esegui (Modalità valutazione)

Consente di eseguire lo scenario selezionato in modalità di valutazione. Fare riferimento all'argomento Funzionamento della replica (a pagina 21).

Sincronizza

Consente di attivare il processo di sincronizzazione (che la replica sia in esecuzione o meno). Per ulteriori informazioni, consultare la sezione Sincronizzazione dei server master e replica (a pagina 131).

Ripristina dati

Consente di recuperare dati perduti o danneggiati sul server master da qualsiasi server di replica attivando un processo di sincronizzazione in direzione inversa. Per ulteriori informazioni, consultare la sezione Recupero di dati e server (a pagina 251).

Rapporto delle differenze

Consente di generare un Rapporto delle differenze, che mostra la differenza tra un server master e i relativi server di replica in un determinato punto nel tempo. Il confronto viene eseguito mediante gli stessi algoritmi utilizzati nel processo di sincronizzazione, ma senza trasferire alcun dato. Per ulteriori informazioni, consultare la sezione Rapporti delle differenze (a pagina 169).

Esegui avanzamento

[Solo per HA] Consente di invertire i ruoli attivo e passivo tra i server master e di replica seguendone lo stato corrente. Per ulteriori informazioni, consultare la sezione Avanzamento (a pagina 259).

Sospensione della verifica Funzionante

[Solo per HA] Consente di sospendere la verifica di funzionamento che controlla se il server attivo è operativo. Per ulteriori informazioni, consultare la sezione Funzionante (a pagina 281).

Aggiorna statistiche

Consente di aggiornare le informazioni sullo stato dello scenario e la visualizzazione delle statistiche live. Per ulteriori informazioni, consultare la sezione Aggiornamento manuale della visualizzazione statistiche (a pagina 163).

Sospensione della replica

Consente di sospendere gli aggiornamenti della replica sull'host di replica allo scopo di eseguire la manutenzione del sistema o qualche altra forma di elaborazione che non modifica i dati ivi replicati. La registrazione delle modifiche continuerà a essere eseguita per l'aggiornamento del server di replica sospeso, ma il trasferimento effettivo non verrà eseguito fino alla ripresa della replica. Non è possibile sospendere la replica durante la sincronizzazione. Per ulteriori informazioni, consultare la sezione Sospensione della replica (a pagina 148).

Verifica di integrità di replica

Consente di eseguire la verifica per Assured Recovery in modalità non pianificata. Per ulteriori informazioni, si rimanda alla sezione Esecuzione della verifica Assured Recovery in modalità non pianificata (a pagina 322).

Avvia/Interrompi computer virtuale

Consente di avviare o interrompere il computer virtuale. L'opzione è applicabile per scenari di recupero o High Availability di dati per scenari di sistema completi.

Elimina tutte le risorse del computer virtuale

Consente di eliminare tutte le risorse temporanee del computer virtuale quali, file di disco, snapshot e altri file temporanei.

Avvia manutenzione host

Consente di preparare un nodo nel sistema replicato per procedure di manutenzione pianificate, evitando di eseguire la risincronizzazione al termine di tali procedure. Per ulteriori informazioni, consultare la sezione Manutenzione host (a pagina 197).

Gestione sincronizzazione non in linea

Consente di specificare la sincronizzazione dei dati blocco per blocco e di avviare il processo di replica.

Configura proxy HTTP

Consente di specificare i dettagli del server proxy per la connessione ai moduli RHA.

Invia un feedback

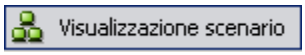
Consente di accedere alla pagina dei commenti e suggerimenti.

Argomenti della Guida in linea

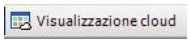
Aprire la Guida in linea.

Barra degli strumenti Visualizzazione

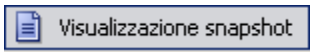
I pulsanti presenti sulla barra degli strumenti di visualizzazione consentono un accesso rapido alle varie finestre e schermate della Gestione. Nell'elenco seguente viene riportata una breve descrizione di ciascuna opzione della barra degli strumenti.



Il pulsante **Visualizzazione scenario** consente di accedere alla schermata principale di Gestione, in cui è possibile creare, monitorare e gestire gli scenari di replica.



La **visualizzazione Cloud** consente la connessione a Amazon EC2 per eseguire la gestione delle istanze.



Il pulsante **Visualizzazione snapshot** consente di accedere alla finestra Gestione VSS, in cui è possibile visualizzare e gestire le snapshot VSS.

Il pulsante **Monitoraggio installazione remota** consente di accedere alla Visualizzazione installazione remota, in cui è possibile visualizzare lo stato dell'installazione dei moduli installati mediante l'installazione remota. Per ulteriori informazioni sull'installazione remota, fare riferimento alla *Guida all'installazione di Arcserve RHA*.

Il pulsante **Monitoraggio manutenzione host** consente di accedere alla finestra Monitoraggio manutenzione host (a pagina 197), in cui è possibile visualizzare lo stato delle richieste correnti per la preparazione alla manutenzione.

Registrazione licenze di Arcserve RHA

Il criterio di licenza di Arcserve RHA si basa su una combinazione di vari parametri che include:

- i sistemi operativi in uso
- la soluzione richiesta
- server applicazioni e database supportati
- il numero degli host coinvolti
- moduli aggiuntivi (per esempio, Assured Recovery)

La chiave di licenza generata per l'utente è adeguata alle sue precise esigenze.

Dopo aver eseguito l'accesso per la prima volta oppure se la licenza è scaduta, sarà necessario registrare il prodotto Arcserve RHA utilizzando la chiave di licenza. Per registrare il prodotto, sarà necessario aprire la Gestione. Per questa operazione non è necessario disporre di una chiave di registrazione valida. Dopo aver avviato la Gestione, verrà visualizzato un avviso di licenza, in cui si richiede di registrare il prodotto. Il messaggio Avviso di licenza verrà visualizzato anche quando la licenza sta per scadere, nel corso dei 14 giorni successivi.

Quando si sta creando uno scenario, alcune delle opzioni potrebbero essere disabilitate in base ai termini della licenza in uso. Prima di eseguire uno scenario specifico, è possibile creare un numero illimitato di scenari, purché la chiave di licenza sia valida. Solo quando si fa clic sul pulsante Esegui, il sistema verifica se l'utente è autorizzato a eseguire lo scenario selezionato in base alla chiave di licenza in uso. Se il sistema determina che l'utente non dispone della licenza richiesta per l'esecuzione di questo scenario, lo scenario non verrà eseguito e si riceverà un messaggio nel riquadro Eventi, che informa l'utente del tipo di licenza necessario.

Per registrare Arcserve RHA mediante la chiave di licenza, procedere come segue:

1. Aprire la Gestione.

   Viene visualizzato un messaggio di benvenuto seguito da un messaggio di avviso di licenza che informa che il prodotto non è registrato. Viene richiesto di effettuare la registrazione del prodotto.

2. Fare clic su OK per chiudere il messaggio.

3. Quindi, aprire il menu della guida in linea e selezionare l'opzione Registra.

   Viene visualizzata la finestra di dialogo Registrazione di Arcserve RHA.

4. Completare i seguenti campi:

   - Campo Chiave di registrazione - immettere la chiave di registrazione.
   - [Facoltativo] Nel campo Nome Azienda - immettere il nome dell'azienda

5. Fare clic sul pulsante Registra per registrare il prodotto e chiudere la finestra di dialogo.

   A questo punto, è possibile iniziare a lavorare con la Gestione Arcserve RHA secondo le proprie autorizzazioni di licenza.

Capitolo 3: Creazione di scenari Replication e High Availability

Arcserve RHA protegge i server nel contesto degli scenari definiti dall'utente. Lo scenario è un'unità operativa di base e consiste in un set di definizioni che include:

- Il tipo di server di applicazioni o database da proteggere.
- Il tipo di soluzione di protezione dei dati.
- Attività speciali, quali Verifica integrità per Assured Recovery.
- I dettagli sulla connessione degli host master e di replica.
- Le directory, sottodirectory, i database e i file che verranno replicati e la relativa posizione sul server master e di replica.
- Le proprietà configurabili dello scenario e degli host master e di replica, che influiscono su diverse impostazioni e operazioni, quali ad esempio il metodo di sincronizzazione, la modalità di replica, la dimensione dello spool, le regole di gestione di rapporti ed eventi e molto altro.
- Parametri di recupero, avanzamento e failover.

Ogni scenario definisce una struttura di replica che imposta il flusso di informazioni dal server master a un dato numero di server di replica. Esso stabilisce la procedura di recupero dei dati e, se applicabili, i parametri di avanzamento. È possibile configurare, aggiungere o rimuovere server da uno scenario e selezionare o modificare directory. Ciò consente di ottenere facilmente il completo controllo del processo di replica su qualsiasi rete, grande o piccola. Ogni scenario viene salvato come file XML. In questa sezione vengono fornite istruzioni sulla creazione di un gruppo di scenari, di uno scenario mediante la Creazione guidata scenario o un modello, e di un modello di scenario.

Questa sezione contiene i seguenti argomenti:

Creazione di uno scenario di replica di file server (a pagina 47)
Creazione di scenari Arcserve Central Host-Based VM Backup (a pagina 57)
Creazione di un nuovo scenario HA per file server (a pagina 66)
Uso dei Gruppi di scenari (a pagina 73)
Utilizzo dei modelli (a pagina 80)
Gestione degli host che utilizzano periferiche NAT (a pagina 86)

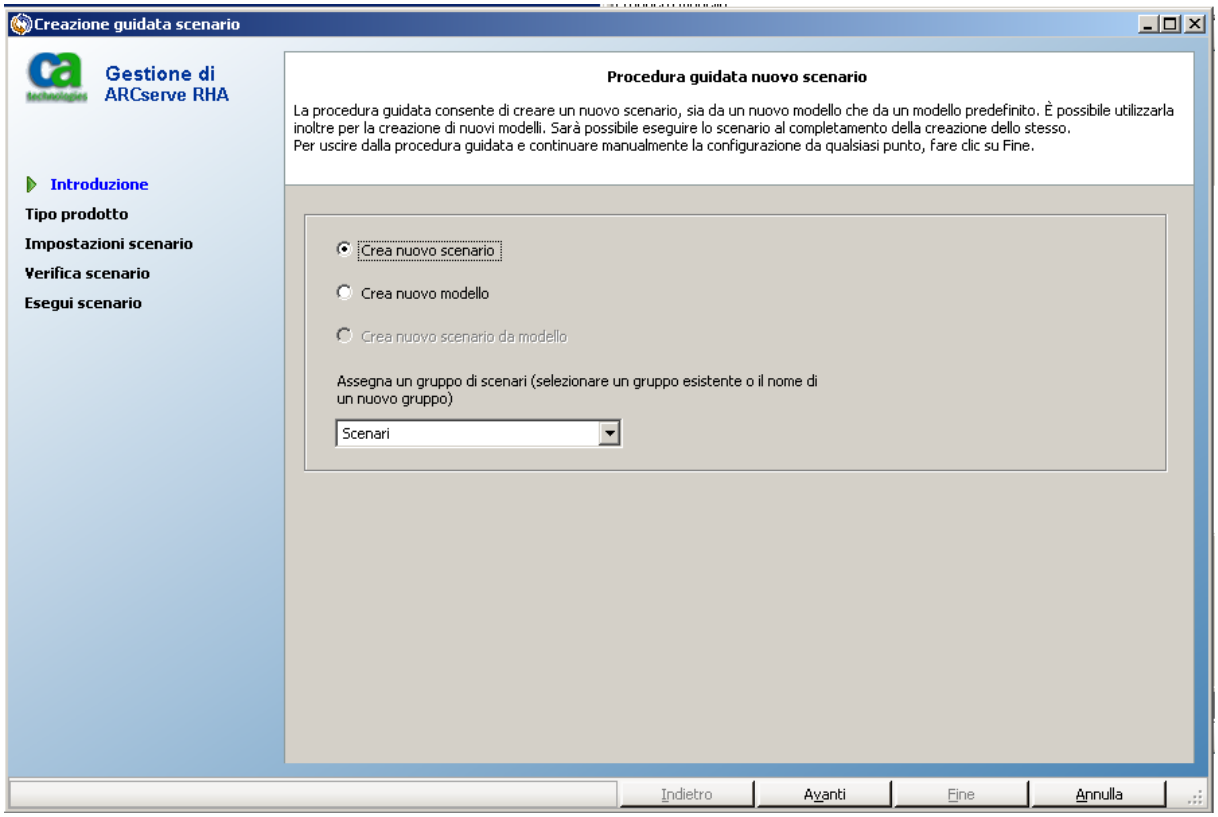
Creazione di uno scenario di replica di file server

La procedura seguente descrive la creazione di uno scenario di replica di file server. Per ulteriori istruzioni sugli scenari personalizzati per applicazioni specifiche, quali server Exchange o SQL, consultare la *Guida operativa di Arcserve RHA* appropriata.

Procedere come descritto di seguito:

1. Aprire la Gestione. Dal menu Scenario, fare clic su Nuovo oppure fare clic sul pulsante Nuovo sulla barra degli strumenti standard.

   Viene visualizzata la schermata Introduzione della Creazione guidata dello scenario .


Creazione guidata scenario
Gestione di ARCserve RHA
Introduzione
Tipo prodotto
Impostazioni scenario
Verifica scenario
Esegui scenario
Procedura guidata nuovo scenario
La procedura guidata consente di creare un nuovo scenario, sia da un nuovo modello che da un modello predefinito. È possibile utilizzarla inoltre per la creazione di nuovi modelli. Sarà possibile eseguire lo scenario al completamento della creazione dello stesso.
Per uscire dalla procedura guidata e continuare manualmente la configurazione da qualsiasi punto, fare clic su Fine.
Crea nuovo scenario
Crea nuovo modello
Crea nuovo scenario da modello
Assegna un gruppo di scenari (selezionare un gruppo esistente o il nome di un nuovo gruppo)
Scenari
Indietro
Avanti
Fine
Annulla

   La schermata Introduzione consente di creare un nuovo scenario e di assegnarlo ad un gruppo di scenari. Dalla schermata Introduzione, è possibile creare un nuovo scenario direttamente, da un modello oppure creare un nuovo modello. Per ulteriori informazioni sulla creazione di modelli, si rimanda alla sezione Utilizzo di modelli. (a pagina 80)

   Nota: Per accedere ad altre funzionalità della Gestione durante la creazione dello scenario, è possibile ridurre a icona la schermata della procedura guidata della creazione dello scenario. La procedura guidata di creazione scenario è associata alla visualizzazione dello scenario. Cambiando visualizzazione, la procedura guidata viene ridotta a icona automaticamente.

2. Selezionare le opzioni necessarie, come riportate di seguito:

   a. Selezionare Crea nuovo scenario

   b. Assegnare lo scenario al gruppo "Scenari" oppure immettere un nome per creare un gruppo.

   c. Fare clic su Avanti.

Viene visualizzata la schermata Selezione del server e del tipo di prodotto.

Questa schermata elenca le applicazioni supportate e i tipi di prodotto disponibili, a seconda della licenza Arcserve RHA di cui si dispone.

3. Selezionare il server richiesto, il tipo di prodotto e le opzioni di integrazione, attenendosi alla seguente procedura:

   a. Dall'elenco Seleziona tipo server, fare clic su File server. Per ulteriori informazioni sugli altri tipi di server, si rimanda alla relativa guida operativa.

   b. Dall'elenco Seleziona tipo prodotto, fare clic su Scenario di replica e recupero dati (DR). Per ulteriori informazioni sugli scenari di High Availability (HA), si rimanda alla sezione Creazione di un nuovo scenario HA di file server (a pagina 66).

   c. Se necessario, selezionare Verifica di integrità per Assured Recovery. Per ulteriori informazioni sulla Verifica integrità per Assured Recovery, si rimanda alla sezione Assured Recovery per file server. (a pagina 25)

   d. Selezionare una delle opzioni seguenti dall'elenco Opzioni di integrazione.

      Nessuno

      Indica che non si desidera includere nella creazione dello scenario i prodotti Arcserve integrati. Fare clic su Avanti.

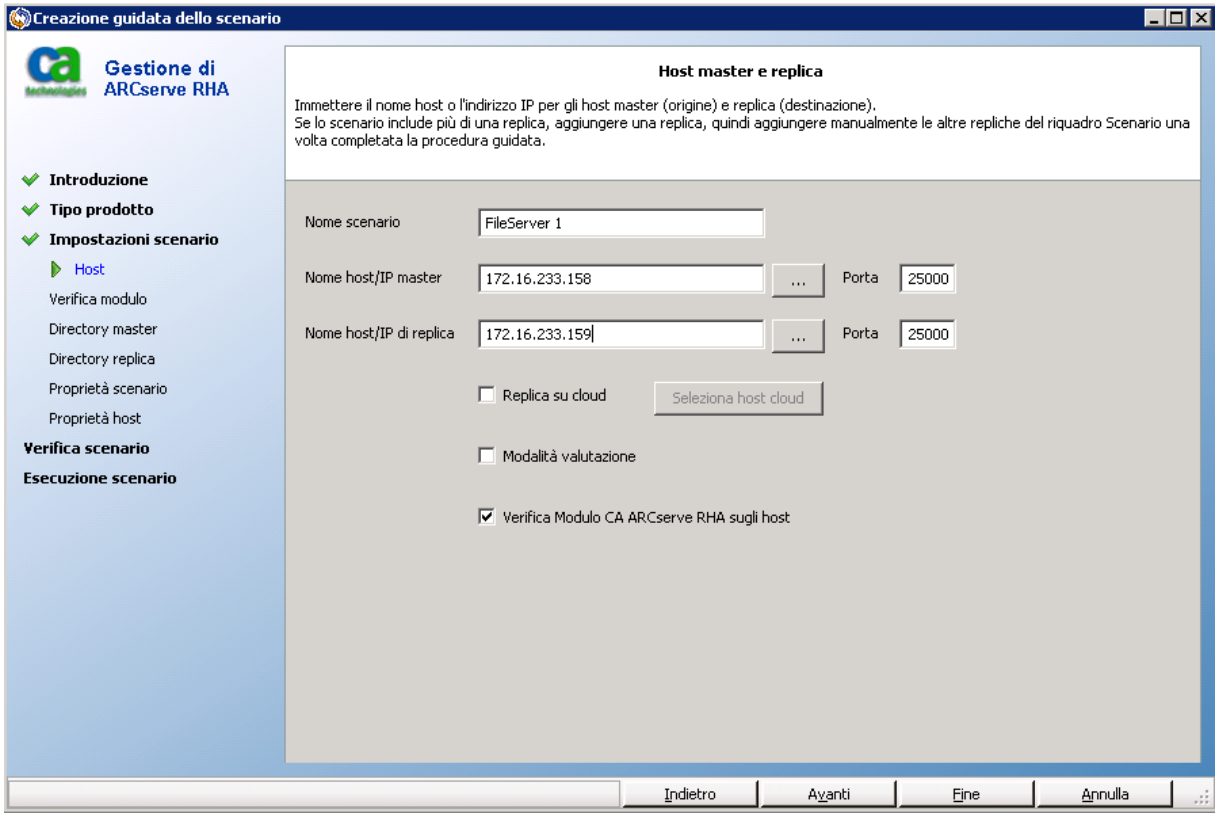
      Arcserve Backup

      Indica che lo scenario utilizza Arcserve Backup per eseguire il backup della replica RHA.

      Immettere il nome del server di backup. Fare clic su Avanti.

      Nota: Per ulteriori informazioni sul backup, consultare la *Guida per l'amministratore* di Arcserve Backup disponibile nel bookshelf di Arcserve Backup.

Viene visualizzata la schermata Host master e replica.



Su questa schermata, specificare l'host da proteggere (Master) e l'host che contiene i dati replicati (Replica).

4. Selezionare gli host master e replica, attenendosi alla procedura seguente:

   a. Nel campo Nome scenario, mantenere il nome predefinito o immetterne uno nuovo.

   b. Nel campo di Nome Host/IP master, immettere il nome host o l'indirizzo IP del server master. Tale server corrisponde al server di origine. Utilizzare il pulsante Sfoglia per individuare un server.

c. Nel campo Nome host/IP di replica, immettere il nome host o l'indirizzo IP del server di replica. Questo server corrisponde al server di destinazione. Utilizzare il pulsante Sfoglia per individuare un server. Se si desidera includere altre repliche nello scenario, immettere i dettagli del primo server o del server padre. Una volta terminata la procedura guidata di creazione scenario, è possibile immettere manualmente ulteriori server di replica. Consultare la sezione Aggiunta di server di replica supplementari (a pagina 173).

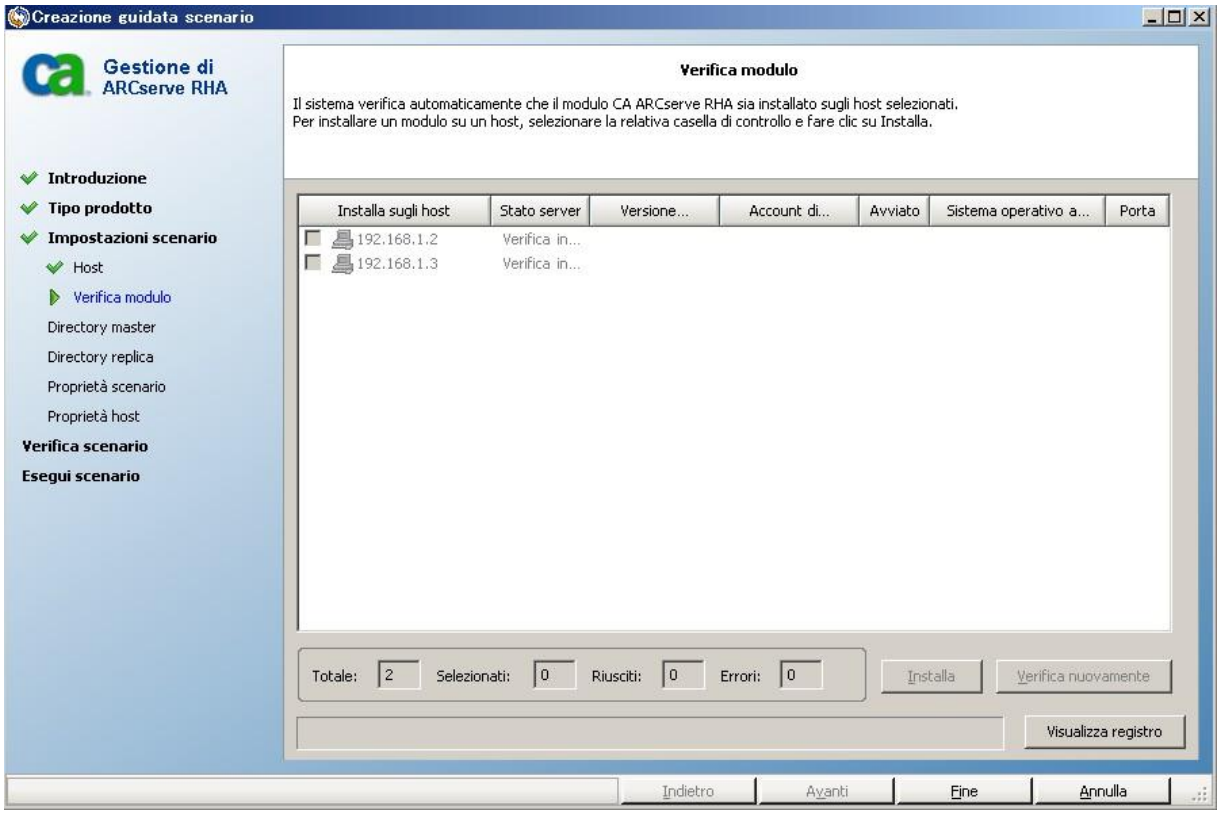
d. Nel campo Porta, mantenere il numero di porta predefinito (25000) o immettere altri numeri di porta per il master e la replica.

e. [Facoltativo] Selezionare la casella di controllo Modalità valutazione se si desidera raccogliere dati statistici accurati sull'utilizzo della larghezza di banda e il benchmarking del rapporto di compressione necessario per la replica, senza in realtà replicare i dati. Se si seleziona questa opzione, la replica non verrà eseguita, e al termine del processo di valutazione verrà fornito un rapporto. Per questo esempio, non abilitare questa opzione.

f. (Facoltativo) Abilitare l'opzione di verifica del modulo Arcserve RHA sugli host per verificare che i moduli siano installati e in esecuzione sugli host master e di replica specificati. Se i Moduli non sono stati installati sugli host specificati è possibile utilizzare questa opzione per l'installazione remota dei Moduli su uno o entrambi gli host. Per questo esempio, abilitare questa opzione.

g. Fare clic su Avanti.

Se l'opzione di verifica del modulo Arcserve RHA sugli host è stata abilitata, verrà visualizzata la schermata di verifica degli host. Il software verifica l'esistenza e la connettività degli host master e replica specificati nella schermata precedente. Al termine, il software esegue un'analisi per controllare se è stata eseguita l'installazione del modulo su ogni host. Se l'accesso alla Gestione viene eseguito con credenziali utente diverse rispetto agli host remoti, lo stato del server viene indicato come Non connesso. Verrà, quindi, richiesto di immettere le credenziali utente per ciascun host selezionato. La verifica verrà eseguita nuovamente.



5. Dalla schermata di verifica degli host, controllare nella colonna Versione corrente se il modulo è stato installato sugli host selezionati.

   Eseguire una delle seguenti operazioni:

   - Se viene visualizzata l'indicazione Installato nella colonna Stato server in entrambe le righe, sarà possibile andare alla pagina successiva.
   - Se viene visualizzata l'indicazione Installato, ma il numero di versione è diverso da quello del Servizio di controllo in uso, installare la versione corrente.
   - Se viene visualizzata l'indicazione Non installato, procedere all'installazione del modulo. Fare clic su Installa per procedere all'installazione del modulo sull'host selezionato. È possibile installare il modulo su entrambi gli host contemporaneamente. Selezionare i server e fare clic su Installa.

     Sarà quindi necessario immettere le credenziali dell'account al servizio del modulo Arcserve RHA.

     - Per gli scenari di replica: è sufficiente essere un amministratore locale (sistema locale).
     - Per i cluster (inclusi gli scenari di replica) è necessario utilizzare lo stesso account del servizio cluster.
     - Per scenari HA, è necessario utilizzare un account con privilegi di amministrazione di dominio nell'ambiente Active Directory, oppure disporre di privilegi di amministrazione locali nell'ambiente del gruppo di lavoro.

   a. Attendere il completamento dell'installazione. Il numero di versione del modulo apparirà nella colonna Versione corrente.

   b. Fare clic su Avanti.

   Viene visualizzata la schermata Directory principali master.

   Questa schermata visualizza le directory e i file presenti sul server master. Si tratta delle directory e dei file che è possibile replicare e proteggere. Il software aggrega automaticamente i dati con percorso comune in un'unica directory.

   Quando si selezionano le directory principali per i server master e di replica,il numero di caratteri utilizzati per i nomi della directory principale e della sottodirectory non deve eccedere i 1024 byte.

6. Dalla schermata Directory principali master, selezionare le directory e i file che si desidera replicare dal master alla replica, facendo clic sulle relative caselle di controllo. Per escludere cartelle e file, deselezionare la casella di controllo corrispondente.

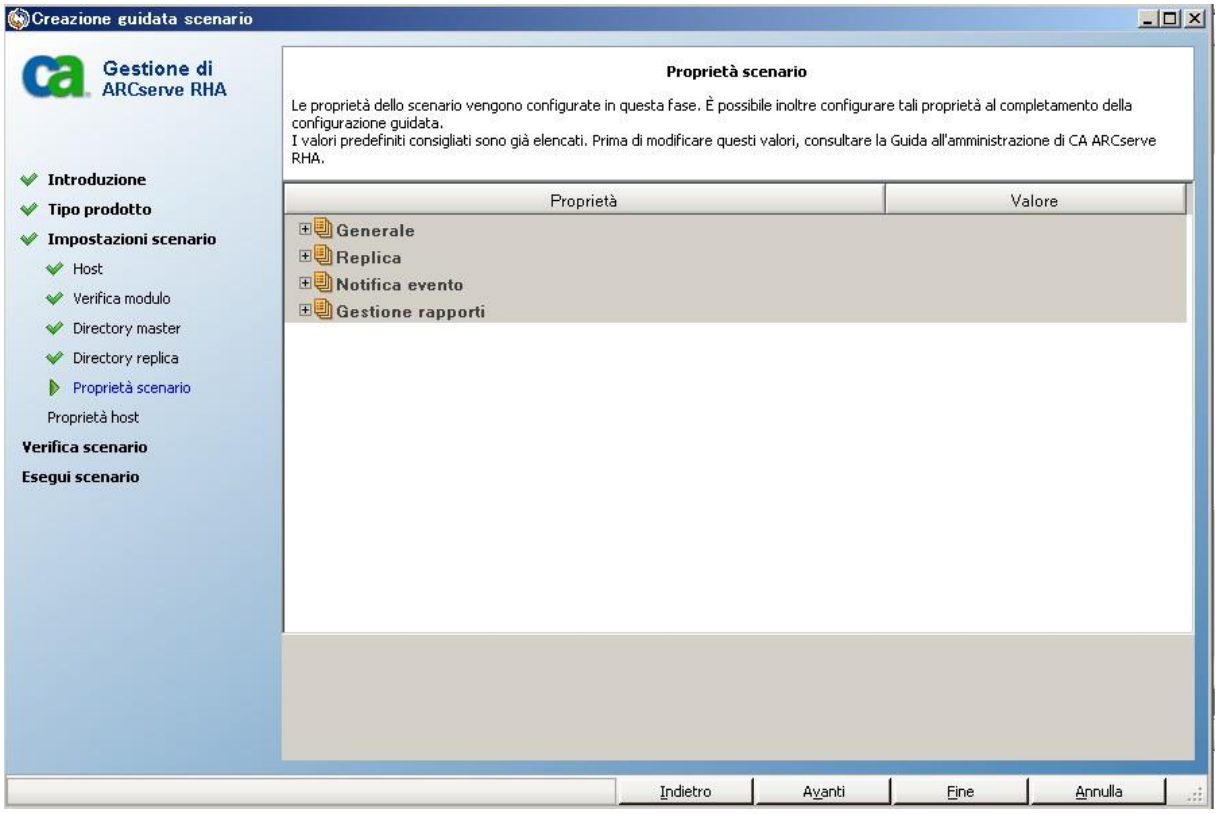
   Quando viene selezionata un'unità o una directory di sinistra, il software ne visualizza i suoi contenuti a destra. Per ulteriori informazioni, si rimanda alla sezione Filtrare file di directory master (a pagina 178).

È possibile eseguire correttamente la replica dei punti di montaggio solo se questi sono stati aggiunti al server master prima dell'esecuzione del modulo. Se i punti di montaggio sono stati inclusi nelle directory principali master quando il modulo era già in esecuzione, non verrà segnalato alcun errore ma la replica non verrà avviata. In tal caso, è necessario riavviare il modulo prima di inizializzare la replica.

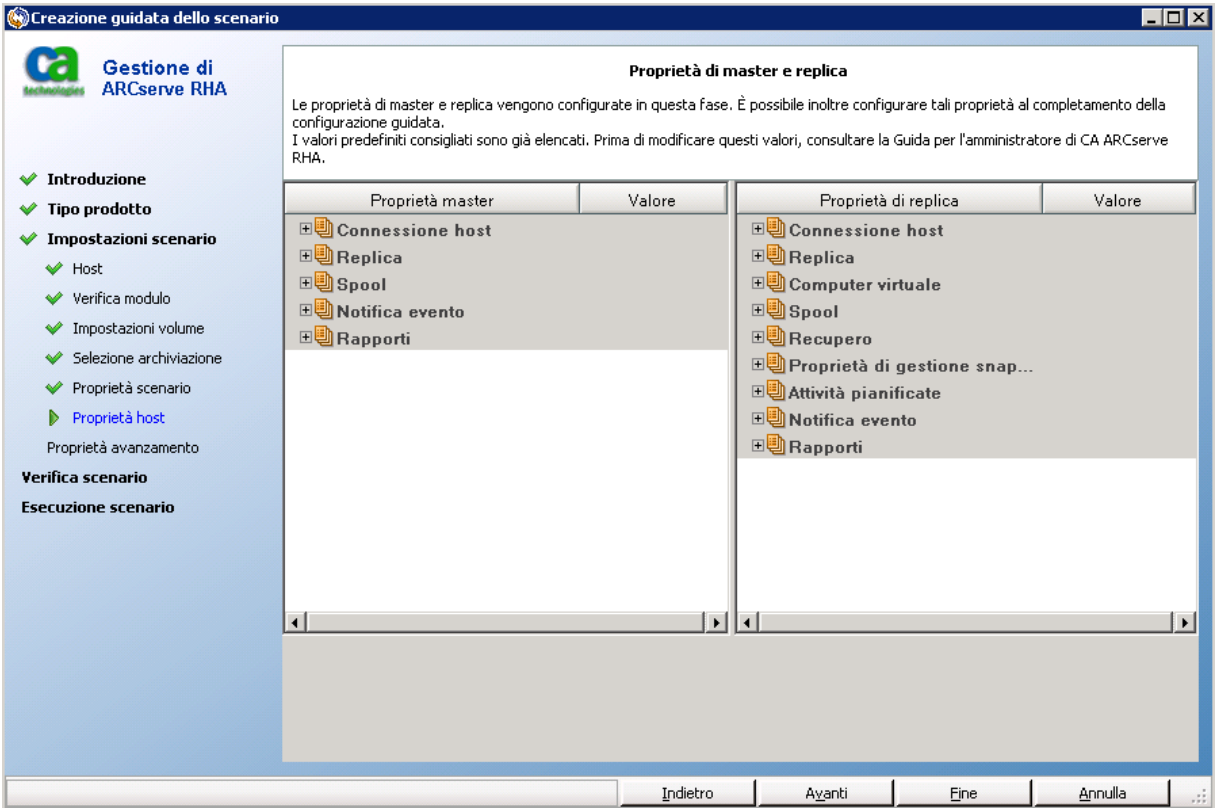
7. Fare clic su Avanti. Viene visualizzata la schermata Directory principali di replica.

   Accettare la directory principale predefinita o digitare un nuovo nome per la directory.

8. Fare clic su Avanti. Viene visualizzata la schermata Proprietà scenario.



9. Nella schermata Proprietà scenario, configurare le proprietà riguardanti l'intero scenario. Per questo esempio, accettare semplicemente le impostazioni predefinite. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni sulla configurazione delle proprietà dello scenario, si rimanda alla sezione Configurazione delle proprietà dello scenario (a pagina 201). Fare clic su Avanti. Viene visualizzata la schermata Proprietà di master e replica.



10. Nella schermata Proprietà di master e replica configurare le proprietà relative all'host master o di replica. Per questo esempio, accettare semplicemente le impostazioni predefinite. Per ulteriori informazioni, si rimanda alla sezione Configurazione delle proprietà del server master e del server di replica (a pagina 216).

    Prima di modificare le proprietà dello spool, è necessario rivedere le informazioni di spool.

    Fare clic su Avanti. Attendere l'apertura della schermata di verifica scenario.

11. Il software convalida il nuovo scenario e ne verifica i parametri per assicurare il completamento corretto della replica. Una volta completata la verifica, la schermata si aprirà e visualizzerà eventuali problemi e avvisi. Il software consente di procedere anche in caso di visualizzazione di avvisi. Risolvere qualunque avviso per garantire una corretta esecuzione del software.

    Fare clic su Avanti quando tutti gli errori e gli avvisi saranno stati risolti. Viene visualizzata la schermata Esecuzione scenario.

12. Con l'esecuzione dello scenario viene avviato il processo di sincronizzazione dei dati. Selezionare Esegui ora per avviare immediatamente la sincronizzazione oppure Fine per salvare la configurazione dello scenario ed inizializzarla in un secondo momento.

    Nota: La sincronizzazione potrebbe richiedere del tempo a seconda delle dimensioni dei dati e della larghezza di banda della rete. Se necessario, selezionare Sincronizzazione non in linea. Per ulteriori informazioni, consultare la sezione Metodi di sincronizzazione (a pagina 18).

    Se si seleziona l'opzione Esegui ora, il software notificherà all'utente il completamento della sincronizzazione. Una volta terminata la sincronizzazione, la replica in tempo reale sarà operativa e lo scenario di replica sarà attivo.

    Verrà generato, quindi, un rapporto di sincronizzazione. Per visualizzare il rapporto, si rimanda alla sezione Visualizzazione di un rapporto (a pagina 167).

Considerazioni sulla creazione di uno scenario Arcserve D2D

Se si seleziona Arcserve D2D come tipo di scenario, tenere presenti le seguenti limitazioni e raccomandazioni:

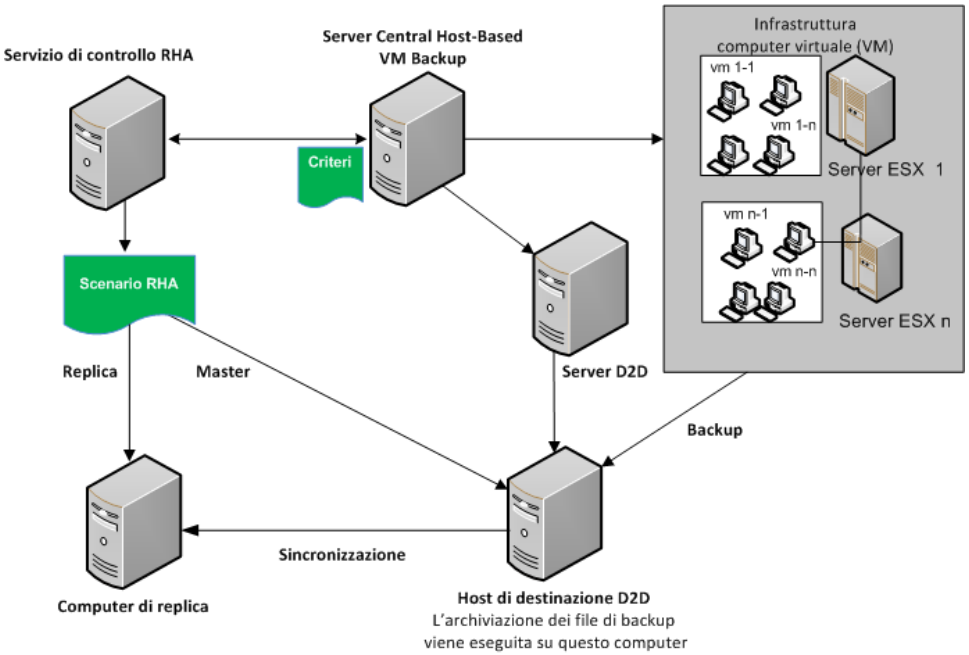
- Se viene modificata la destinazione di D2D e viene aggiornato lo scenario Arcserve RHA con la nuova destinazione, le sessioni precedenti sulla replica andranno perse dopo la sincronizzazione. Ciò si verifica perché le sessioni precedenti non esistono sulla nuova destinazione di D2D.
- Se la destinazione di D2D è un disco locale, verificare che lo spool Arcserve RHA sia configurato su un volume non protetto da Arcserve D2D. In caso contrario, Arcserve D2D eseguirà il backup dei file diario archiviati nello spool Arcserve RHA.

Creazione di scenari Arcserve Central Host-Based VM Backup

Arcserve RHA consente di proteggere file di backup multipli creati da Arcserve D2D. Per proteggere i file di backup multipli, è necessario utilizzare il server Arcserve Central Host-Based VM Backup.

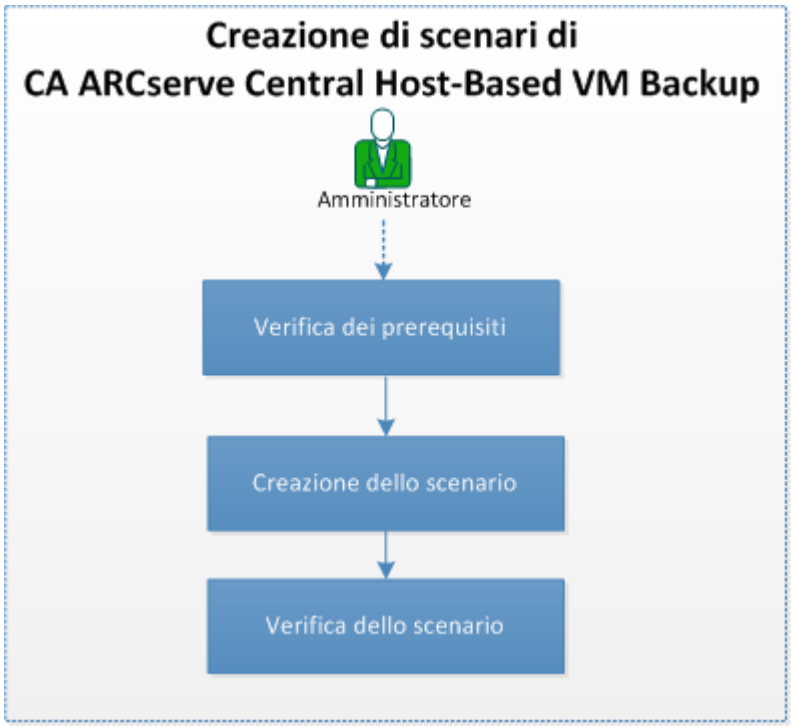
Nell'installazione mostrata di seguito, il server Arcserve Central Host-Based VM Backup utilizza Arcserve D2D per eseguire il backup di computer virtuali multipli. Tali file di backup vengono archiviati sugli host D2D. Per proteggere i file di backup, il Servizio di controllo RHA esegue la connessione al server Central Host-Based VM Backup e acquisisce i dettagli dell'host D2D. L'host D2D archivia i file di backup. Selezionare quindi i file di backup che si desidera proteggere e creare uno scenario per la replica di tali file di backup di D2D.

Il diagramma seguente mostra le impostazioni di un'installazione che include RHA, D2D e Central Host-Based VM Backup.



Per proteggere file di backup multipli (creati da Arcserve D2D), creare uno scenario di Central Host-Based VM Backup. Specificare le credenziali del server Arcserve Central Host-Based VM Backup e selezionare i computer virtuali dal server host D2D.

Il diagramma seguente mostra il processo di creazione di uno scenario di Arcserve Central Host-Based Backup.



Per creare uno scenario Arcserve Central Host-Based Backup, effettuare le attività seguenti:

1. Verifica dei prerequisiti (a pagina 59)
2. Creazione dello scenario (a pagina 59)
3. Verifica dello scenario (a pagina 66)

Verifica dei prerequisiti

Assicurarsi di verificare i seguenti prerequisiti prima di creare lo scenario di Arcserve Central Host-Based VM Backup.

- Arcserve D2D è stato installato e l'ambiente di backup è stato configurato. Per informazioni su Arcserve D2D, consultare la *Guida per l'utente di Arcserve D2D.*
- Arcserve Central Host-Based VM Backup (HBBU) è installato e il server Central Host-Based VM Backup è in grado di accedere ai server D2D. Per informazioni su Arcserve Central Host-Based VM Backup, consultare la *Guida per l'utente di Arcserve Central Host-Based VM Backup.*
- L'utente è ora in grado di creare scenari file server di RHA.

Creazione dello scenario

Creare lo scenario di integrazione Central Host-Based VM Backup per eseguire la replica dei file di backup creati da Arcserve.

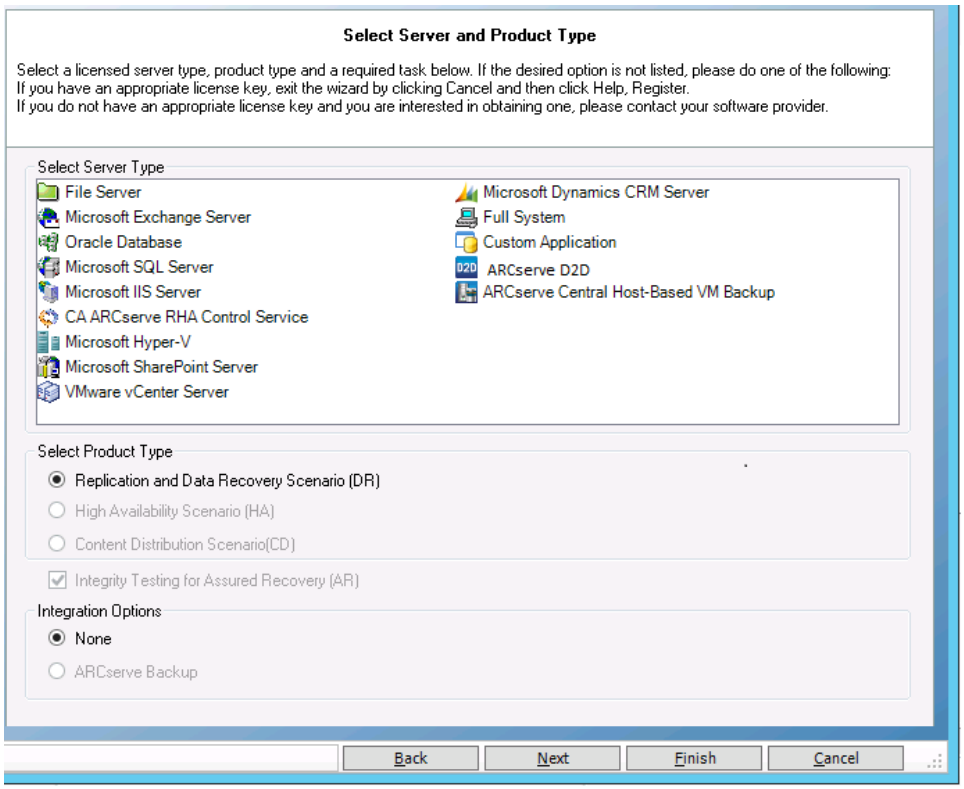
Procedere come descritto di seguito:

1. Aprire la Gestione. Dal menu Scenario, fare clic su Nuovo oppure fare clic sul pulsante Nuovo della barra degli strumenti standard.

   Viene visualizzata la schermata Introduzione della Creazione guidata dello scenario .

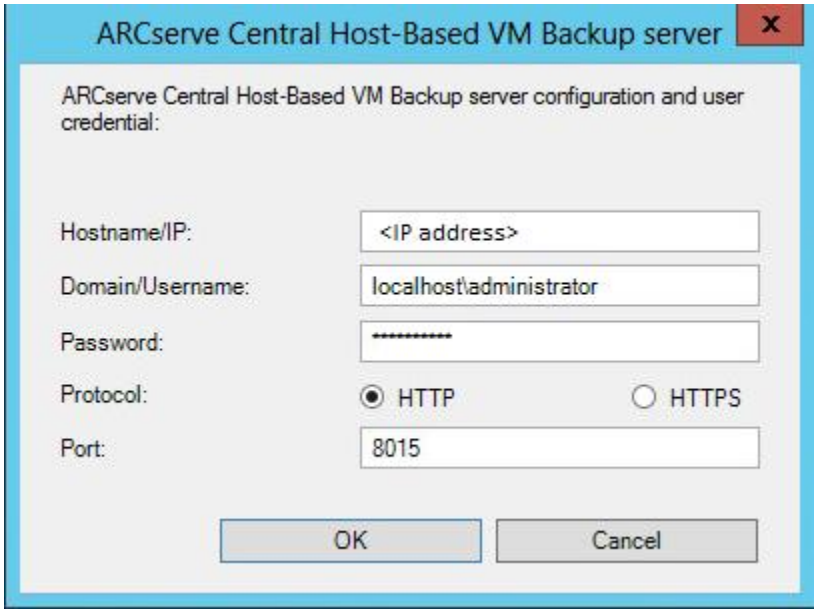
2. Selezionare Crea nuovo scenario

Viene visualizzata la schermata Selezione del server e del tipo di prodotto.


Select Server and Product Type
Select a licensed server type, product type and a required task below. If the desired option is not listed, please do one of the following:
If you have an appropriate license key, exit the wizard by clicking Cancel and then click Help, Register.
If you do not have an appropriate license key and you are interested in obtaining one, please contact your software provider.
Select Server Type
File Server
Microsoft Exchange Server
Oracle Database
Microsoft SQL Server
Microsoft IIS Server
CA ARCserve RHA Control Service
Microsoft Hyper-V
Microsoft SharePoint Server
VMware vCenter Server
Microsoft Dynamics CRM Server
Full System
Custom Application
ARCserve D2D
ARCserve Central Host-Based VM Backup
Select Product Type
Replication and Data Recovery Scenario (DR)
High Availability Scenario (HA)
Content Distribution Scenario(CD)
Integrity Testing for Assured Recovery (AR)
Integration Options
None
ARCserve Backup
Back
Next
Finish
Cancel

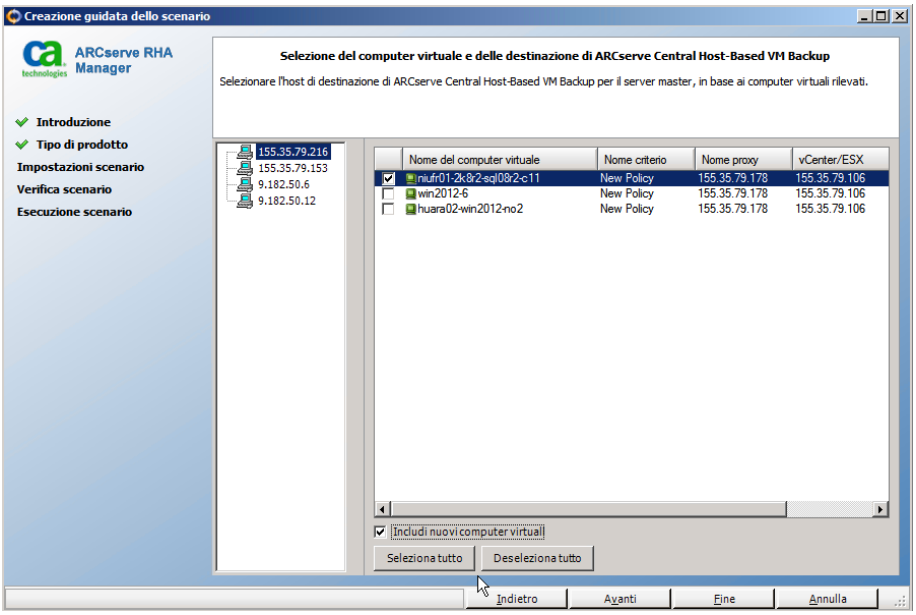
3. Selezionare le opzioni seguenti e fare clic su Avanti.
   a. Tipo server: Arcserve Central Host-Based VM Backup.
   b. Tipo di prodotto: Scenario di replica e recupero dati (DR).
   c. Opzioni di integrazione: Nessuno.

Viene visualizzata la finestra delle credenziali del server Arcserve Central Host-Based VM Backup.



4. Immettere le credenziali del server Central Host e fare clic su OK. Il nome del server viene compilato in base ai dati specificati nel passaggio 3.

   Viene visualizzata la schermata Selezione del computer virtuale e delle destinazione di Arcserve Central Host-Based VM Backup.



Arcserve RHA esegue la connessione al server Central Host-Based Backup per acquisire il criterio e visualizzare gli host di destinazione di backup e i computer virtuali corrispondenti.

5. Selezionare il nome host e i computer virtuali che si desiderano proteggere.

   Includi nuovi computer virtuali: specifica la replica di tutte le sottocartelle contenute nella cartella di backup dell'host principale quando si esegue questo scenario. Vengono inoltre replicate tutte le cartelle di backup dei computer virtuali appena create. Sono escluse solo le cartelle dei computer virtuali non selezionate. Tali cartelle vengono contrassegnate come da escludere. Se non si seleziona questa opzione, vengono replicate solo le cartelle di backup selezionate.

   I file di backup dei computer virtuali selezionati vengono replicati durante l'esecuzione dello scenario. Si tratta dei file di backup creati da Arcserve D2D.

6. Immettere i seguenti dati per il master e la replica:

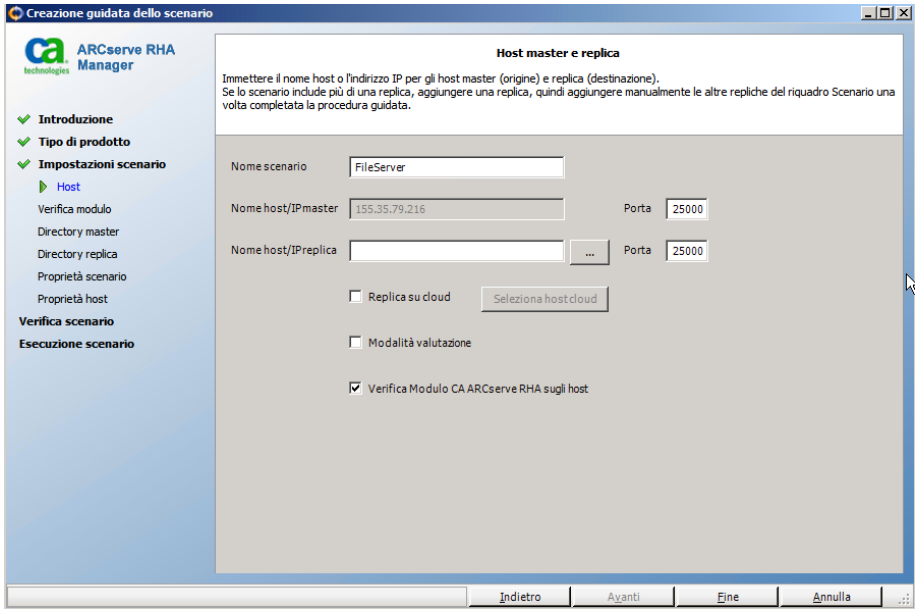
   Nome scenario: accettare il nome predefinito o immetterne un nome univoco.

   Nome host/IP master: questo campo viene compilato automaticamente in base al nome host selezionato.

   Nome host/IP di replica: immettere il nome host o l'indirizzo IP del server di replica. Questo server corrisponde al server di destinazione. Utilizzare il pulsante Sfoglia per individuare un server.

   Porta: accettare il numero di porta predefinito (25000) o immettere altri numeri di porta per il master e la replica.

   (Facoltativo) Verifica Modulo Arcserve RHA sugli host: consente di verificare che i moduli siano installati e in esecuzione sugli host master e di replica specificati.



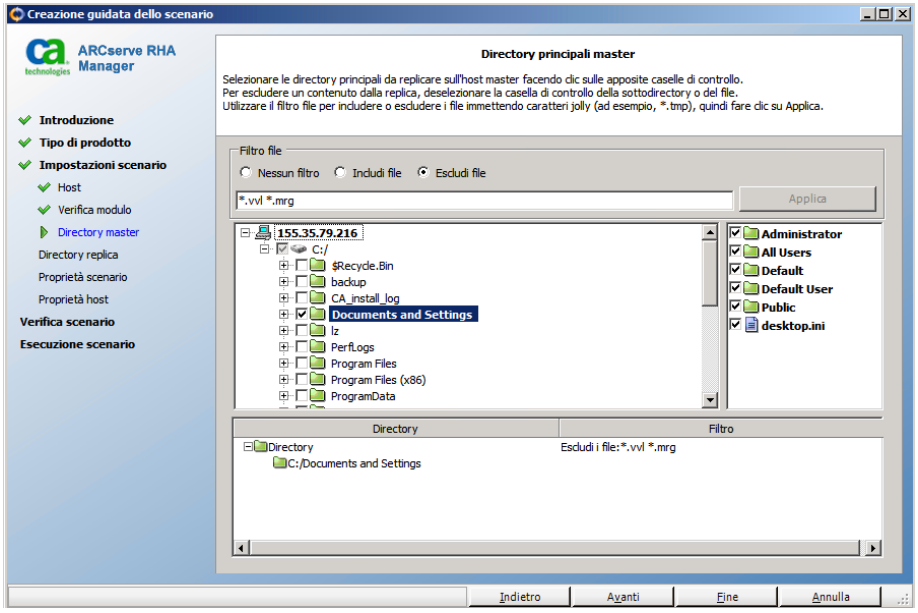
7. Fare clic su Avanti.

   Viene visualizzata la schermata Verifica modulo.

   Se l'opzione Verifica Modulo Arcserve RHA sugli host è stata abilitata, verrà visualizzata la relativa schermata. Il software verifica l'esistenza e la connettività degli host master e replica specificati nella schermata precedente.

8. Fare clic su Avanti.

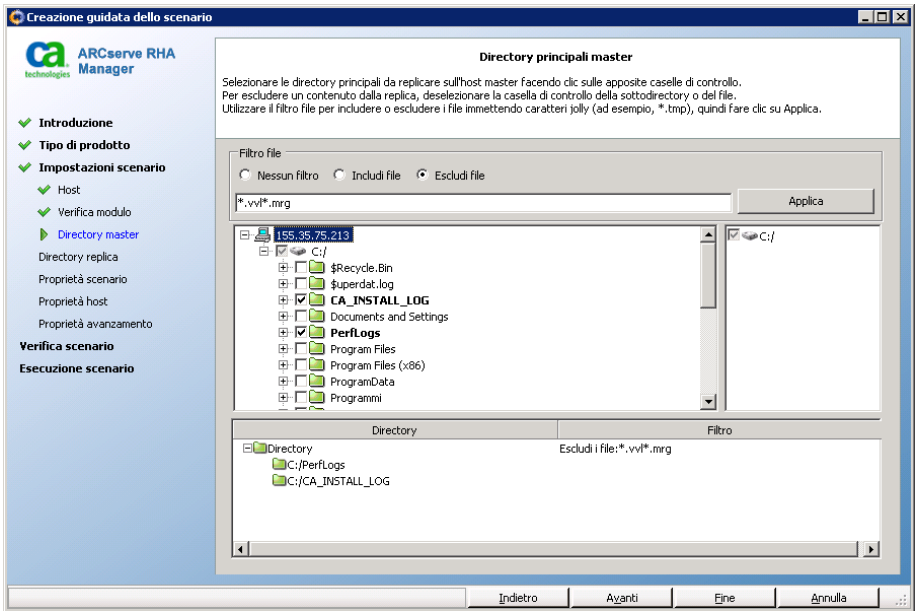
   Viene visualizzata la schermata Directory principali master.



   Il modulo RHA rileva le cartelle di backup dei computer virtuali selezionati. Le cartelle di backup vengono selezionate automaticamente.

   Nota: queste cartelle corrispondono alle cartelle di backup create da Arcserve D2D.

Quando si seleziona l'opzione Includi nuovi computer virtuali nella schermata Selezione del computer virtuale e della destinazione di ArcserveCentral Host-Based VM Backup, la cartella di backup principale viene selezionata per la replica, mentre le cartelle escluse vengono elencate nel riquadro di filtro.



9. Fare clic su Avanti.

   Viene visualizzata la schermata Directory principali di replica.

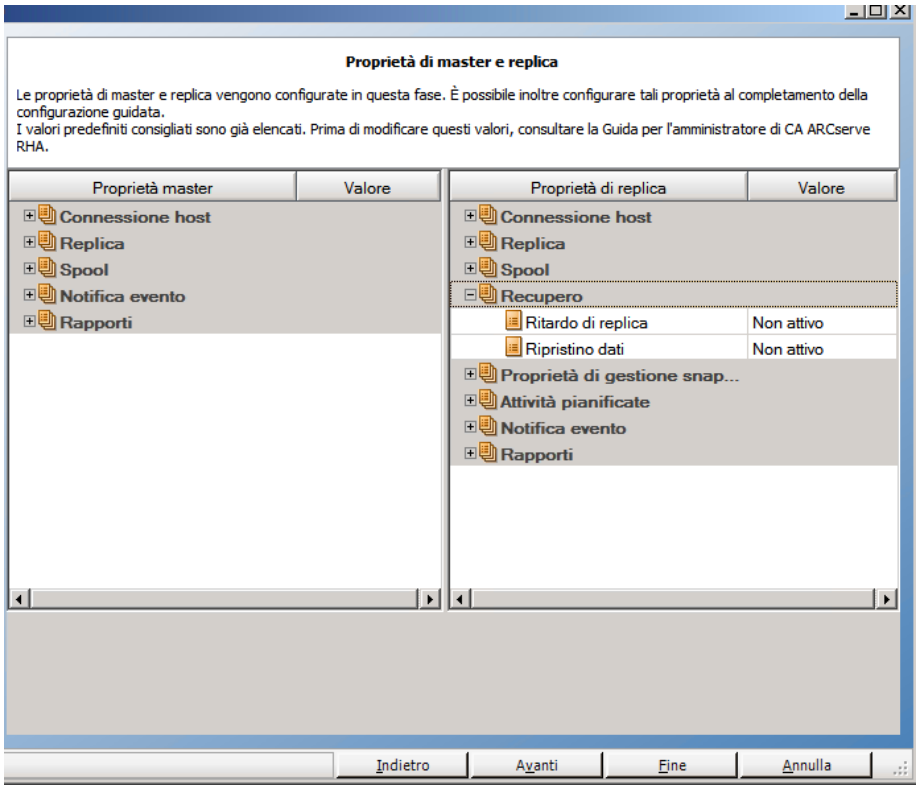
10. Accettare le impostazioni predefinite e fare clic su Avanti.

    Viene visualizzata la schermata Proprietà scenario.

11. Configurare le proprietà riguardanti l'intero scenario. Per questo esempio, accettare semplicemente le impostazioni predefinite. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni sulla configurazione delle proprietà dello scenario, consultare la sezione Configurazione delle proprietà di uno scenario (a pagina 201).

12. Fare clic su Avanti.

    Viene visualizzata la schermata Proprietà di master e replica.



13. Configurare le proprietà relative agli host master o di replica. Per questo esempio, accettare semplicemente le impostazioni predefinite. Per ulteriori informazioni sulla configurazione delle proprietà del master e della replica, consultare la sezione Configurazione delle proprietà del server master o di replica (a pagina 216).

14. Fare clic su Avanti.

    Viene visualizzata la schermata Verifica scenario.

    Il software convalida il nuovo scenario e ne verifica i parametri per assicurare il completamento corretto della replica. Una volta completata la verifica, la schermata si aprirà e mostrerà eventuali problemi e avvisi. Il software consente di procedere anche in caso di visualizzazione di avvisi. Se necessario, risolvere gli avvisi.

15. Fare clic su Avanti quando tutti gli errori e gli avvisi saranno stati risolti.

    Viene visualizzata la schermata Esecuzione scenario.

16. Selezionare Fine.

Lo scenario Arcserve Host-Based VM Backup viene creato correttamente. È ora possibile eseguire questo scenario ed eseguire il backup dei file del computer virtuale creati da Arcserve D2D.

Verifica dello scenario

Dopo la creazione dello scenario ArcserveCentral Host-Based VM Backup, lo scenario viene elencato in Gestione RHA, Visualizzazione scenario. Verificare che lo scenario e i dettagli corrispondenti siano inclusi nell'elenco Visualizzazione scenario.

Creazione di un nuovo scenario HA per file server

Prima di avviare questa procedura, leggere la sezione relativa al reindirizzamento IP (a pagina 285) ed eseguire i passaggi prerequisiti necessari per la protezione del proprio ambiente. Se si decide di utilizzare il metodo di reindirizzamento IP di spostamento, è necessario aggiungere un nuovo indirizzo IP alla scheda NIC del server master prima di creare degli scenari.

Tale procedura avvia la creazione guidata degli scenari HA, che guida l'utente attraverso i vari passaggi necessari. È possibile configurare le proprietà senza utilizzare la procedura guidata.

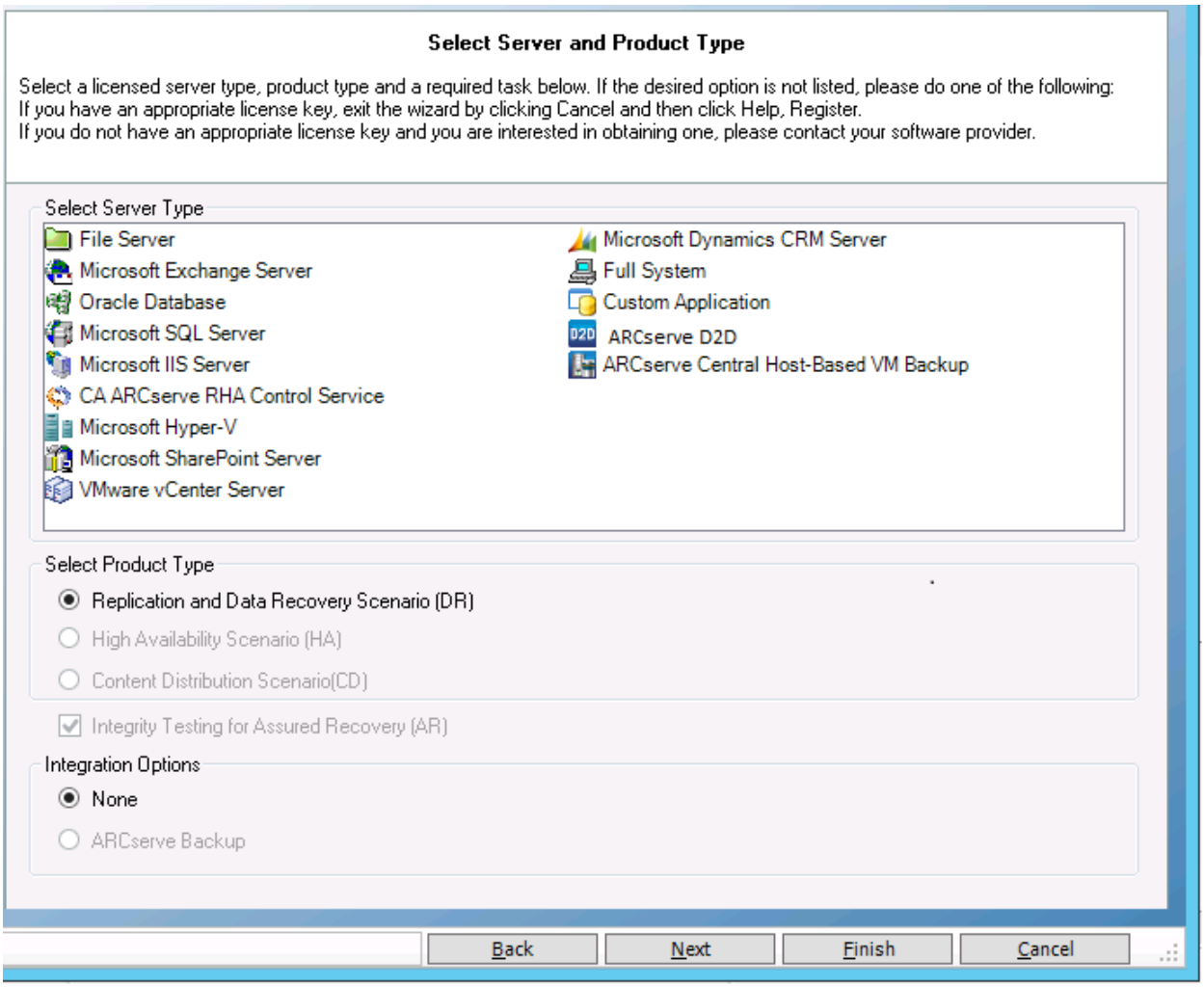
Per creare un nuovo scenario HA di file server:

1. Aprire la Gestione, selezionare Scenario, Nuovo oppure fare clic sul pulsante Nuovo scenario per avviare la creazione guidata.

   Viene visualizzata la finestra di dialogo iniziale.

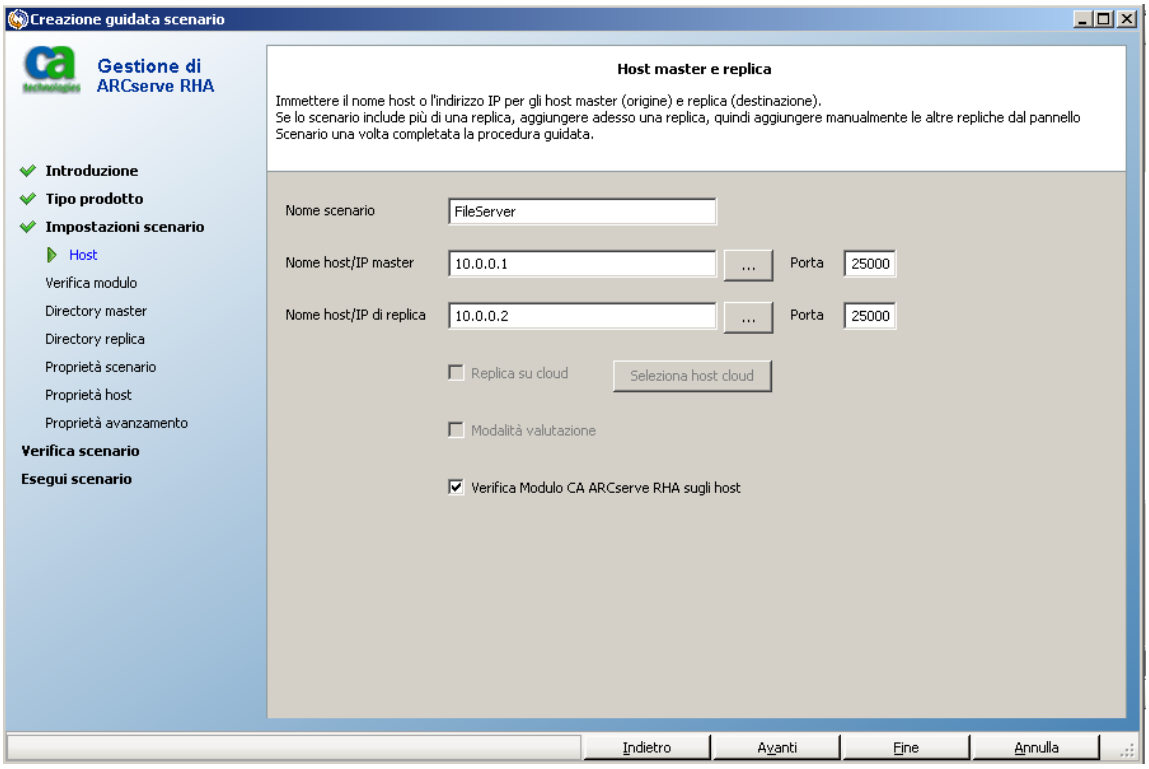
2. Scegliere Crea nuovo scenario, selezionare un gruppo dall'elenco e fare clic su Avanti.

   Viene visualizzata la finestra di dialogo Seleziona server e tipo di prodotto.

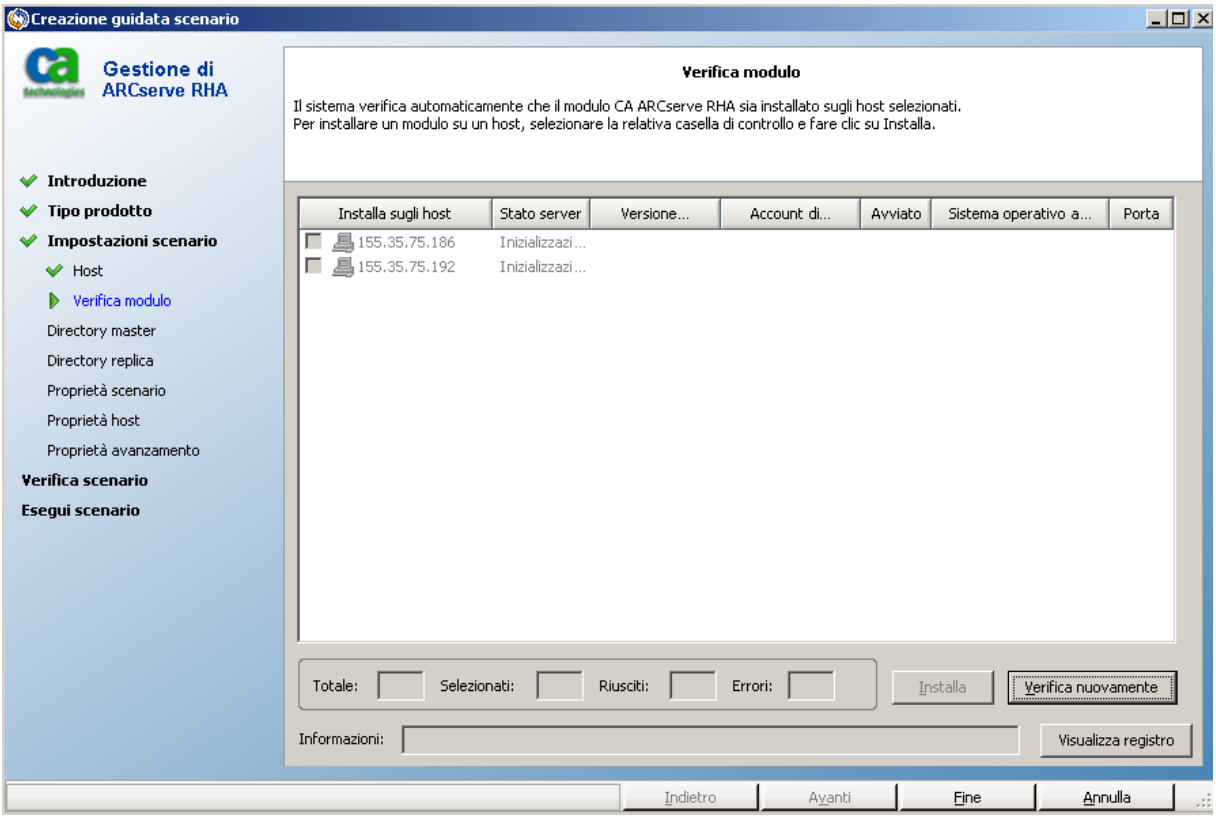

Select Server and Product Type
Select a licensed server type, product type and a required task below. If the desired option is not listed, please do one of the following:
If you have an appropriate license key, exit the wizard by clicking Cancel and then click Help, Register.
If you do not have an appropriate license key and you are interested in obtaining one, please contact your software provider.
Select Server Type
File Server
Microsoft Exchange Server
Oracle Database
Microsoft SQL Server
Microsoft IIS Server
CA ARCserve RHA Control Service
Microsoft Hyper-V
Microsoft SharePoint Server
VMware vCenter Server
Microsoft Dynamics CRM Server
Full System
Custom Application
ARCserve D2D
ARCserve Central Host-Based VM Backup
Select Product Type
Replication and Data Recovery Scenario (DR)
High Availability Scenario (HA)
Content Distribution Scenario(CD)
Integrity Testing for Assured Recovery (AR)
Integration Options
None
ARCserve Backup
Back
Next
Finish
Cancel

3. Scegliere File Server, Scenario High Availability (HA) e fare clic su Avanti.

   Viene visualizzata la finestra di dialogo Host master e replica.



4. Immettere un nome per lo scenario, il nome host o l'indirizzo IP e il numero della porta per i server master e di replica, assicurarsi che l'opzione Verifica Modulo Arcserve RHA sugli host sia abilitata, quindi fare clic su Avanti.



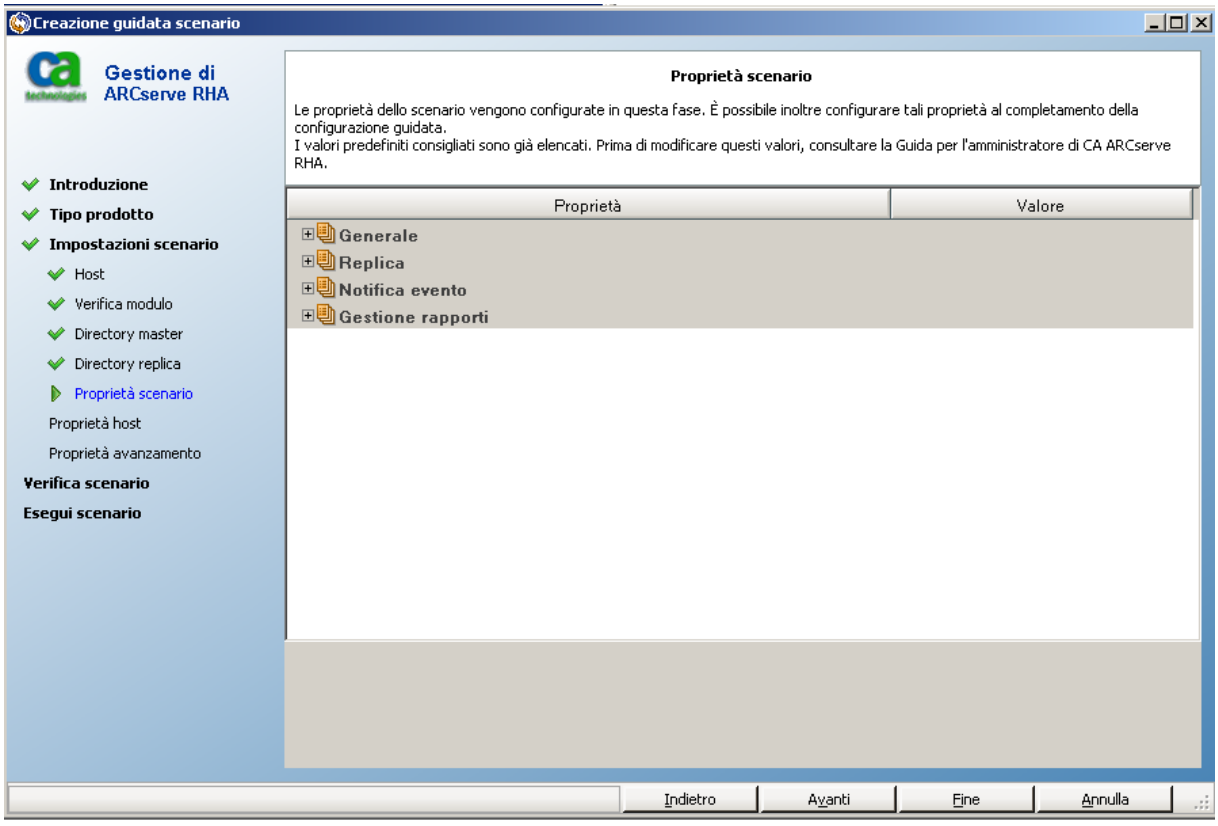
5. Attendere il completamento della verifica modulo e fare clic su Avanti. Se necessario, fare clic su Installa per aggiornare il modulo su uno o su entrambi i server, quindi fare clic su Verifica nuovamente.

   Verrà visualizzata la finestra di dialogo Directory principali master con un elenco delle directory rilevate automaticamente. Per impostazione predefinita nessuna opzione è selezionata. Espandere le cartelle e selezionare il dati che si desidera proteggere. Non è possibile selezionare tutti i file di sistema che vengono esclusi per impostazione predefinita.

6. Fare clic su Avanti. Viene visualizzata la schermata Directory principali di replica.

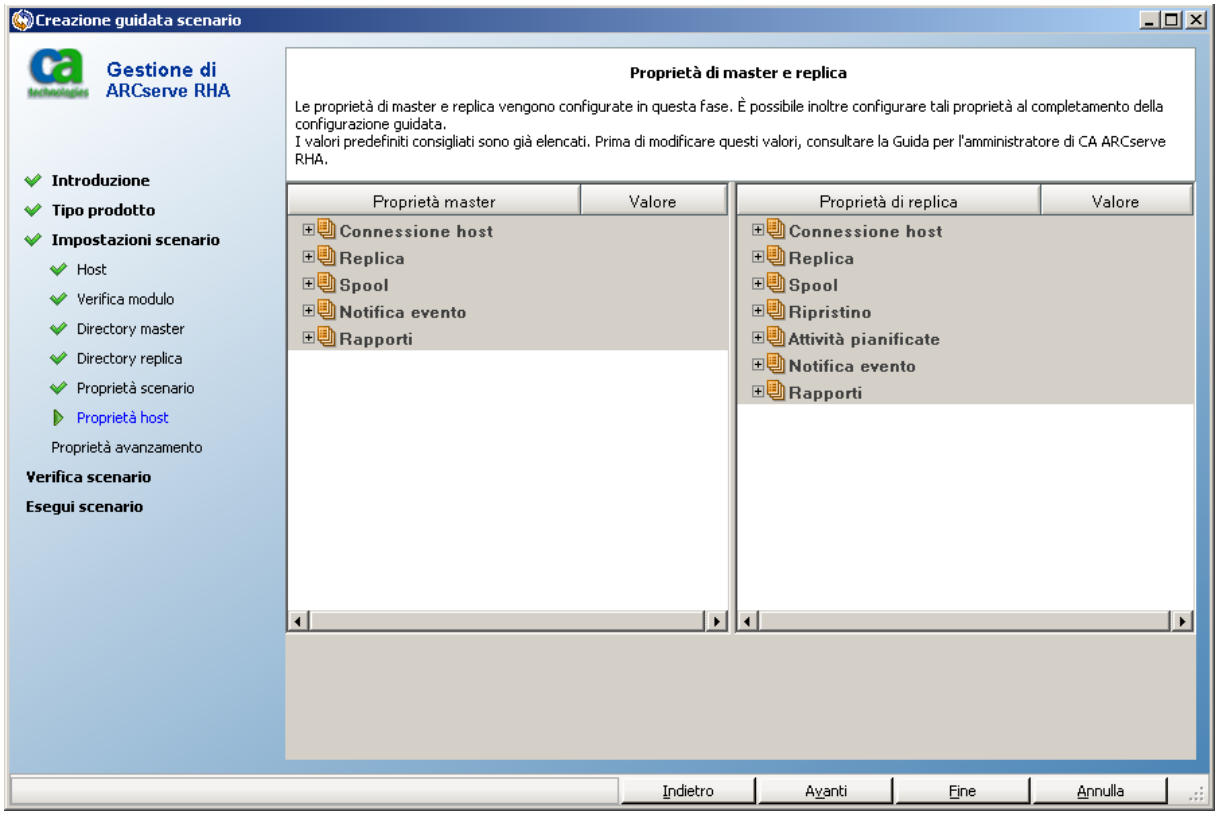
   Accettare la directory principale predefinita o digitare un nuovo nome.

7. Fare clic su Avanti. Viene visualizzata la finestra di dialogo Proprietà scenario.



8. Le proprietà dello scenario controllano l'intero scenario. Accettare i valori predefiniti o i nuovi valori impostati. Al termine dell'operazione, fare clic su Avanti. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni, si rimanda alla sezione Configurazione delle proprietà dello scenario

   Viene visualizzata la finestra di dialogo Proprietà di master e replica.

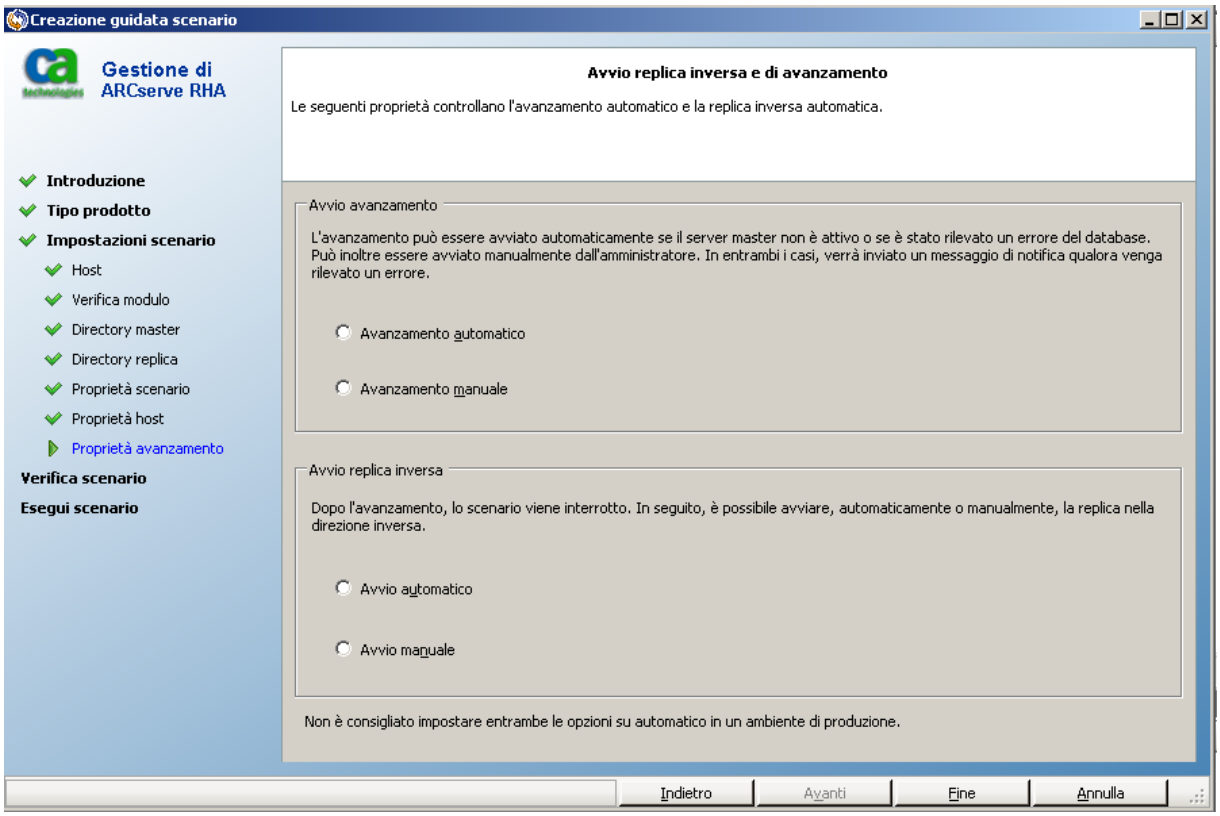


9. Le proprietà del server master e di replica si applicano esclusivamente ai server host. Confermare i valori predefiniti o modificarli, in base alle esigenze. Fare clic su Avanti.

   Recuperare i dati nella finestra di dialogo Proprietà avanzamento che verrà visualizzata.

10. Impostare il metodo di Reindirizzamento traffico di rete desiderato, come descritto nella sezione Reindirizzamento IP. Fare clic su Avanti.

    Viene visualizzata la finestra di dialogo Avvio replica inversa e di avanzamento.


Creazione guidata scenario
Gestione di ARCserve RHA
Introduzione
Tipo prodotto
Impostazioni scenario
Host
Verifica modulo
Directory master
Directory replica
Proprietà scenario
Proprietà host
Proprietà avanzamento
Verifica scenario
Esegui scenario
Avvio replica inversa e di avanzamento
Le seguenti proprietà controllano l'avanzamento automatico e la replica inversa automatica.
Avvio avanzamento
L'avanzamento può essere avviato automaticamente se il server master non è attivo o se è stato rilevato un errore del database. Può inoltre essere avviato manualmente dall'amministratore. In entrambi i casi, verrà inviato un messaggio di notifica qualora venga rilevato un errore.
Avanzamento automatico
Avanzamento manuale
Avvio replica inversa
Dopo l'avanzamento, lo scenario viene interrotto. In seguito, è possibile avviare, automaticamente o manualmente, la replica nella direzione inversa.
Avvio automatico
Avvio manuale
Non è consigliato impostare entrambe le opzioni su automatico in un ambiente di produzione.
Indietro
Avanti
Fine
Annulla

11. Scegliere le opzioni di avvio desiderate. Per gli scenari relativi al file server, impostare l'avvio manuale della replica inversa. Non è consigliabile impostare l'avvio automatico. Per ulteriori informazioni, consultare la sezione Considerazioni sull'avanzamento. Fare clic su Avanti.

    Attendere il completamento della verifica scenario.

12. Se vengono segnalati errori o avvisi, risolverli prima di continuare. Una volta completate le operazioni, fare clic su Avanti.

    Viene visualizzata la finestra di dialogo Esecuzione scenario.

13. Fare clic su Esegui ora per avviare la sincronizzazione e attivare lo scenario oppure su Fine per eseguire lo scenario in un secondo momento.

Uso dei Gruppi di scenari

Ad ogni scenario viene assegnato un gruppo scenari predefinito denominato **Scenari**. È possibile utilizzare questo gruppo per tutti gli scenari creati oppure aggiungere nuovi gruppi per organizzare i propri scenari secondo le proprie necessità. I gruppi di scenari verranno visualizzati sia nella Gestione sia nella Pagina con informazioni introduttive.

In ambienti di server distribuiti, in cui molti server (server di database, server di applicazione, server front-end Web) costituiscono l'ambiente, è necessario creare scenari individuali per proteggere tutti i server della distribuzione. Se una verifica Funzionante attiva un failover, solo il server interessato viene sostituito dal server di replica corrispondente. La consequenziale separazione dei dati, in virtù della quale alcune operazioni vengono applicate ai server master originali ed altre ai server di replica in scenari con errori, può comportare problemi di prestazioni.

I gruppi di scenari consentono di gestire gli scenari corrispondenti come una singola entità, come ad esempio gli scenari che proteggono tutti i server presenti in un ambiente distribuito. Per esempio, per una protezione end-to-end in un ambiente server distribuito, può essere necessario disporre di uno scenario SQL per proteggere il componente di database e di diversi scenari specifici dell'applicazione per proteggere i server applicazione. Un gruppo di scenari consente di impostare le proprietà di avanzamento al livello del gruppo, invece che a livello del singolo server.

Per ulteriori informazioni, si rimanda alla sezione Abilitazione della gestione di gruppi di scenari (a pagina 76) e alla Guida operativa relativa alla specifica applicazione server distribuita.

Nota: per server farm SharePoint, la creazione di gruppi di scenari viene gestita automaticamente. Per altri ambienti di server distribuiti (BlackBerry Enterprise Server e Microsoft Dynamics CRM), è necessario creare i gruppi e gli scenari manualmente.

Passaggi successivi:

- Creazione di un gruppo di scenari (a pagina 74)
- Abilitazione della gestione di gruppi di scenari (a pagina 76)
- Esecuzione di un gruppo di scenari
- Interruzione di un gruppo di scenari (a pagina 80)

Creazione di un gruppo di scenari

Esistono due modi per creare un gruppo di scenari:

- Durante la creazione di un nuovo scenario, utilizzando la Creazione guidata scenario (a pagina 47).
- Prima della creazione di uno scenario, mediante l'opzione **Nuovo gruppo**, come descritto di seguito.

Nota: si consiglia di pianificare e creare in anticipo i gruppi di scenari che si desidera utilizzare. Una volta assegnato uno scenario a un determinato gruppo, non sarà possibile spostarlo in un altro gruppo.

Per creare un nuovo gruppo di scenari, procedere come segue:

1. Dalla Gestione fare clic su Scenario e su Nuovo Gruppo dal menu, oppure fare clic sul pulsante Nuovo gruppo nella barra degli strumenti standard.

   La cartella Nuovo gruppo viene aggiunta al riquadro Scenario.

2. È possibile modificare il nome del gruppo facendo clic con il pulsante destro del mouse su di esso e selezionando Rinomina dal menu di scelta rapida, oppure facendo doppio clic sul nome corrente e immettendone uno nuovo.

   Il nome del nuovo gruppo viene visualizzato nelle seguenti posizioni: il riquadro Scenario, l'elenco a discesa Gruppo nella Creazione guidata scenario e nella Pagina con informazioni introduttive.

   Nota: quando non viene definito alcuno scenario, i gruppi di scenari vuoti non verranno visualizzati nella Pagina con informazioni introduttive.

Impostazione delle proprietà del gruppo

Configurare le proprietà del gruppo dalla scheda Proprietà di gestione di Arcserve RHA.

Le proprietà del gruppo includono:

Elementi dipendenti dallo scenario

Gestisce le relazioni di interdipendenza tra scenari. Di solito un'applicazione distribuita dispone di componenti/ruoli/server multipli interdipendenti. È possibile configurare qualsiasi scenario come elemento dipendente da uno o più scenari oppure scenari multipli come elementi dipendenti da un unico scenario. Tali servizi possono essere gestiti dalla proprietà Elementi dipendenti dallo scenario.

Impostazioni di avanzamento

Gestisce le impostazioni dell'avanzamento in un gruppo distribuito. Alcune delle opzioni dell'impostazione di avanzamento includono:

- Avanzamento come gruppo: se questa opzione è impostata a Attivo, l'avanzamento verrà eseguito automaticamente per l'intero gruppo (tutti gli scenari) se uno degli scenari riporta errori ed è pronto per l'avanzamento.
- Attivazione avanzamento da errore di completamento: un errore singolo può attivare un avanzamento del gruppo. Per impostazione predefinita, tutti gli scenari possono attivare l'avanzamento di un gruppo. È possibile configurare alcuni scenari a bassa densità e impostarli su Non attivo.
- Esegui impostazioni di avanzamento scenario: questa opzione consente di determinare se lo scenario dovrà eseguire le proprie impostazioni di avanzamento.

Set disponibilità scenario

In un'applicazione distribuita è possibile configurare due o più server che forniscano gli stessi servizi per migliorare la disponibilità o le prestazioni del servizio. Quando un server non è disponibile, gli altri server saranno in funzione e potranno così fornire i servizi. Il set di scenari disponibili verrà utilizzato quando Arcserve RHA gestisce i server/gli scenari dell'applicazione distribuita.

Se due scenari sono configurati nello stesso set di scenari disponibili, si procederà all'avanzamento del gruppo solo quando entrambi gli scenari non possono essere completati. Questa funzione non viene richiamata quando una delle opzioni non può essere completata.

Nota: in uno stesso gruppo possono essere presenti uno o più set di disponibilità scenario, ma uno scenario non può essere configurato in due set differenti.

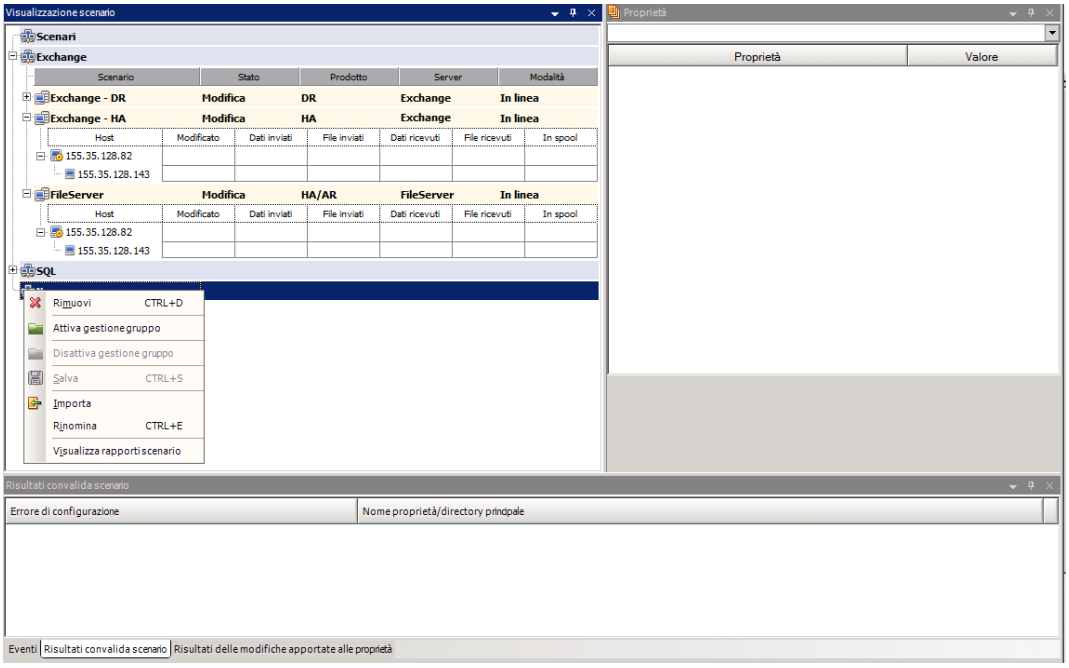
Abilitazione della gestione di gruppi di scenari

La gestione di gruppi di scenari consente di gestire scenari connessi ad HA come entità singole. L'avanzamento può essere configurato in modo tale che quando un server riporta errori, tutti i server nel gruppo degli scenari avanzino contemporaneamente, evitando il problema della dispersione dei dati (a pagina 73). La gestione di gruppi di scenari si applica solo a scenari High Availability.

Nota: per scenari farm di SharePoint Server, la creazione di gruppi e la gestione centrale degli scenari vengono abilitate automaticamente durante la creazione dello scenario. Per ulteriori informazioni, si rimanda alla *Guida operativa di SharePoint Server.* Per tutti gli altri ambienti distribuiti, è necessario creare manualmente gli scenari necessari, assegnare ciascuno di essi ad uno stesso gruppo e abilitare la gestione di gruppo.

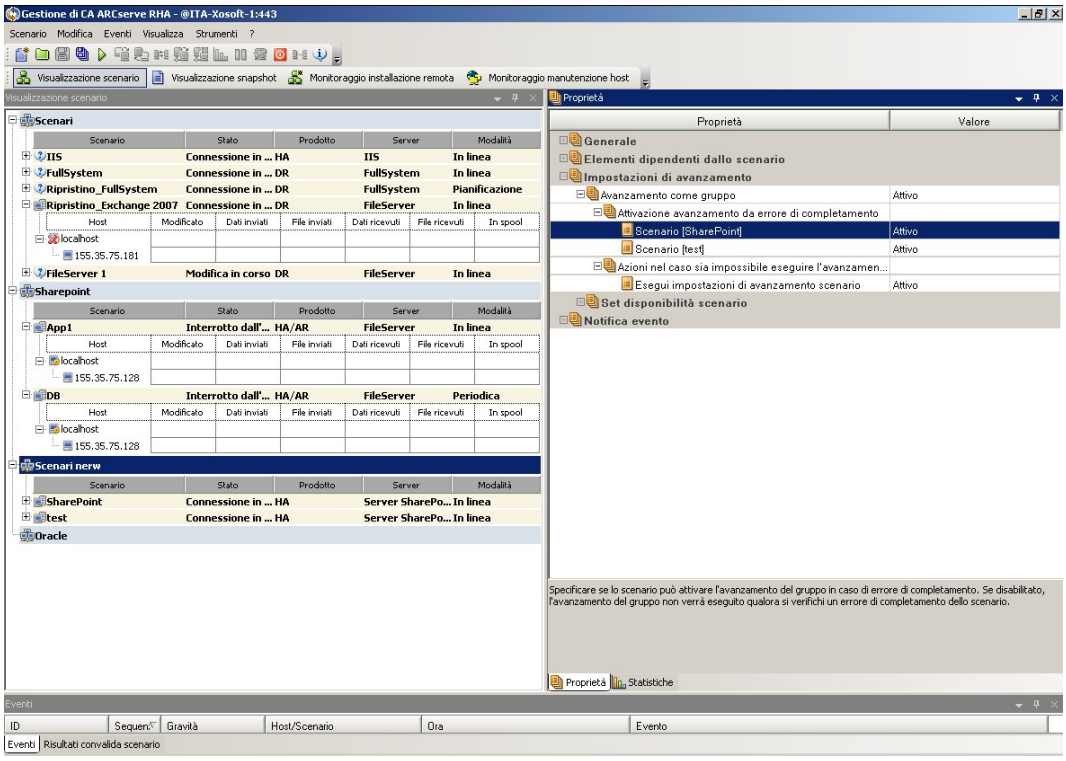
Per abilitare la gestione di gruppi di scenari:

1. Dalla Gestione, fare clic con il tasto destro del mouse sul nome del gruppo di scenario che si desidera gestire in modo centralizzato.
2. Dal menu di scelta rapida, fare clic sull'opzione per l'abilitazione della gestione di gruppi di scenari.

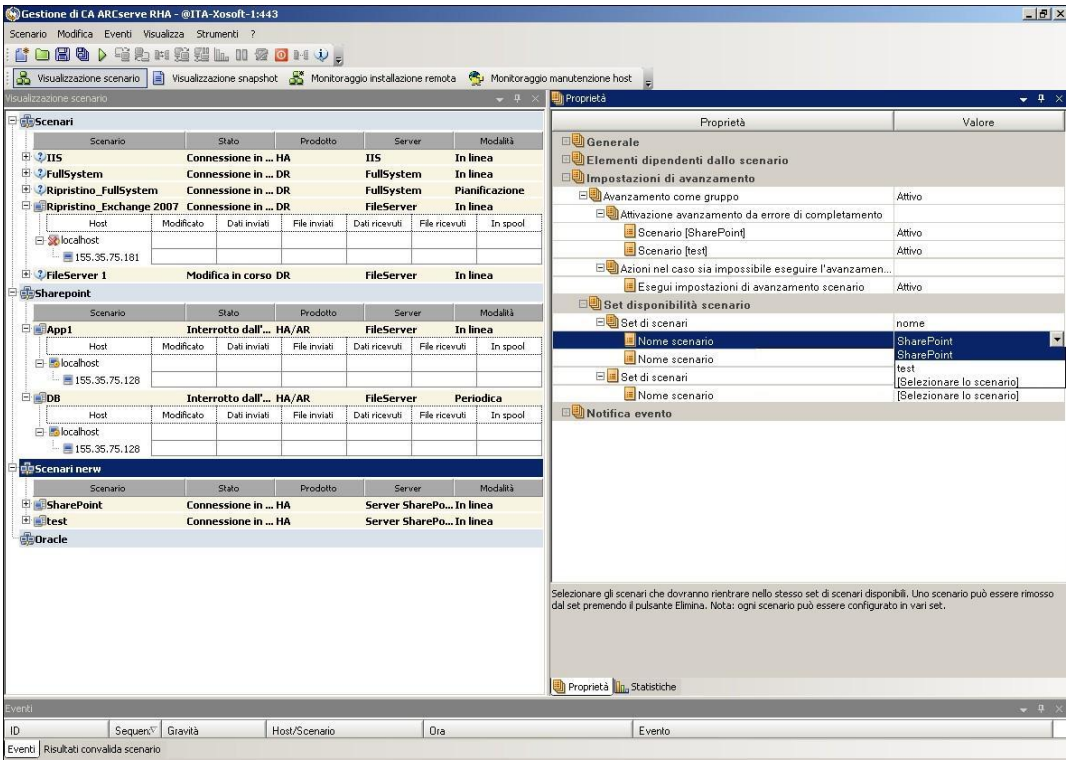


Verrà visualizzato un messaggio di conferma. Fare clic su OK per continuare.

3. Fare clic sulla scheda Proprietà ed espandere il gruppo di proprietà Impostazioni di avanzamento.
4. Se si desidera procedere all'avanzamento dell'intero gruppo come entità singola, impostare la proprietà Avanzamento come gruppo su Attivo.
5. Espandere la proprietà Attivazione avanzamento da errore di completamento e impostare il valore su Attivo per ciascuno scenario nel gruppo che dovrebbe attivare l'avanzamento.


Gestione di CA ARCserve RHA - @ITA-Xosoft-1:443
Scenario Modifica Eventi Visualizza Strumenti ?
Visualizzazione scenario
Visualizzazione snapshot
Monitoraggio installazione remota
Monitoraggio manutenzione host
Visualizzazione scenario
Scenari
Scenario Stato Prodotto Server Modalità
IIS Connessione in ... HA IIS In linea
FullSystem Connessione in ... DR FullSystem In linea
Ripristino_FullSystem Connessione in ... DR FullSystem Pianificazione
Ripristino_Exchange 2007 Connessione in ... DR FileServer In linea
Host Modificato Dati inviati File inviati Dati ricevuti File ricevuti In spool
localhost
155.35.75.181
FileServer 1 Modifica in corso DR FileServer In linea
Sharepoint
App1 Interrotto dall'... HA/AR FileServer In linea
localhost
155.35.75.128
DB Interrotto dall'... HA/AR FileServer Periodica
localhost
155.35.75.128
Scenari nerw
SharePoint Connessione in ... HA Server SharePo... In linea
test Connessione in ... HA Server SharePo... In linea
Oracle
Proprietà
Proprietà Valore
Generale
Elementi dipendenti dallo scenario
Impostazioni di avanzamento
Avanzamento come gruppo Attivo
Attivazione avanzamento da errore di completamento
Scenario [SharePoint] Attivo
Scenario [test] Attivo
Azioni nel caso sia impossibile eseguire l'avanzamen...
Esegui impostazioni di avanzamento Attivo
Set disponibilità scenario
Notifica evento
Specificare se lo scenario può attivare l'avanzamento del gruppo in caso di errore di completamento. Se disabilitato, l'avanzamento del gruppo non verrà eseguito qualora si verifichi un errore di completamento dello scenario.
Proprietà
Statistiche
Eventi
ID Sequen Gravità Host/Scenario Ora Evento
Eventi
Risultati convalida scenario

6. Espandere la proprietà Set disponibilità scenario. Se tutti i server elencati sotto questa proprietà riportano errori, verrà effettuato l'avanzamento dell'intero gruppo. Aggiungere i nomi del gruppo di scenari che si desidera monitorare, quindi selezionare gli scenari di quel gruppo che attiveranno l'avanzamento del gruppo.


Gestione di CA ARCserve RHA - @ITA-Xosoft-1:443
Scenario Modifica Eventi Visualizza Strumenti ?
Visualizzazione scenario
Visualizzazione snapshot
Monitoraggio installazione remota
Monitoraggio manutenzione host
Visualizzazione scenario
Scenari
Scenario Stato Prodotto Server Modalità
IIS Connessione in ... HA IIS In linea
FullSystem Connessione in ... DR FullSystem In linea
Ripristino_FullSystem Connessione in ... DR FullSystem Pianificazione
Ripristino_Exchange 2007 Connessione in ... DR FileServer In linea
Host Modificato Dati inviati File inviati Dati ricevuti File ricevuti In spool
localhost
155.35.75.181
FileServer 1 Modifica in corso DR FileServer In linea
Sharepoint
App1 Interrotto dall'... HA/AR FileServer In linea
155.35.75.128
DB Interrotto dall'... HA/AR FileServer Periodica
Scenari nerw
SharePoint Connessione in ... HA Server SharePo... In linea
test Connessione in ... HA Server SharePo... In linea
Oracle
Proprietà
Proprietà Valore
Generale
Elementi dipendenti dallo scenario
Impostazioni di avanzamento
Avanzamento come gruppo Attivo
Attivazione avanzamento da errore di completamento
Scenario [SharePoint] Attivo
Scenario [test] Attivo
Azioni nel caso sia impossibile eseguire l'avanzamen...
Esegui impostazioni di avanzamento scenario Attivo
Set disponibilità scenario
Set di scenari nome
Nome scenario SharePoint
Nome scenario SharePoint
Set di scenari test
Nome scenario [Selezionare lo scenario]
Notifica evento
Selezionare gli scenari che dovranno rientrare nello stesso set di scenari disponibili. Uno scenario può essere rimosso dal set premendo il pulsante Elimina. Nota: ogni scenario può essere configurato in vari set.
Proprietà Statistiche
Eventi
ID Sequen Gravità Host/Scenario Ora Evento
Eventi Risultati convalida scenario

Esecuzione di un gruppo di scenari

Prima di procedere all'esecuzione di un gruppo di scenari, Arcserve RHA esegue la verifica di pre-esecuzione di ogni scenario del gruppo e riporta qualsiasi errore o avviso riscontrato. È necessario che ogni scenario del gruppo superi la verifica, altrimenti non sarà possibile procedere all'esecuzione del gruppo.

Per ulteriori informazioni, consultare la sezione Esecuzione del processo di replica (a pagina 127).

Per eseguire un gruppo di scenari:

1. Se la verifica di pre-esecuzione viene completata con successo, fare clic su Esegui ora per eseguire il gruppo intero.

   Viene visualizzata la finestra di dialogo Esegui.

2. Scegliere un metodo di sincronizzazione e fare clic su OK. Per impostazione predefinita, il metodo di sincronizzazione del gruppo utilizza il metodo selezionato individualmente per ogni scenario. È anche possibile scegliere di applicare un unico metodo a tutti gli scenari.

   Lo stato per tutti gli scenari del gruppo viene modificato in In esecuzione.

Interruzione di un gruppo di scenari

Per aggiungere o rimuovere scenari è necessario interrompere il gruppo in esecuzione. Per interrompere un gruppo, interrompere tutti gli scenari del gruppo. Fare clic su Interrompi nella barra degli strumenti della Gestione per ogni scenario in sequenza. Non è stato registrato nessun errore durante l'interruzione degli scenari.

Per ulteriori informazioni, consultare la sezione Interruzione della replica (a pagina 131).

Utilizzo dei modelli

I modelli costituiscono una potente funzionalità per la personalizzazione di Arcserve RHA nell'ambiente in uso. Molte applicazioni consentono di effettuare la modifica dei valori predefiniti di singoli parametri. Alcuni esempi potrebbero essere il tipo di carattere predefinito da utilizzare nei nuovi documenti in Microsoft Word oppure la firma predefinita per i nuovi messaggi in un'applicazione client di posta elettronica. I modelli consentono di sviluppare questo concetto:

piuttosto che offrire un metodo per modificare un singolo valore predefinito globale, i modelli offrono la capacità di creare un intero scenario da utilizzare come punto di partenza per nuovi scenari in futuro. Tali scenari di modelli speciali contengono tutti i parametri di uno scenario reale, che sono tutti modificabili, tranne quelli che chiaramente si applicano a uno specifico scenario individuale(ad esempio i nomi host dei server master e di replica).

Il secondo importante vantaggio dei modelli rispetto a un set di valori predefiniti globali è rappresentato dalla possibilità di creare diversi set di valori predefiniti per diversi tipi di scenari. Ad esempio, i valori predefiniti appropriati per gli scenari Exchange High Availability non sono identici a quelli degli scenari di replica di un file server. Con i modelli è possibile creare impostazioni predefinite e mantenerle individualmente per ciascun tipo di scenario richiesto dal proprio ambiente IT.

Creazione di un nuovo modello

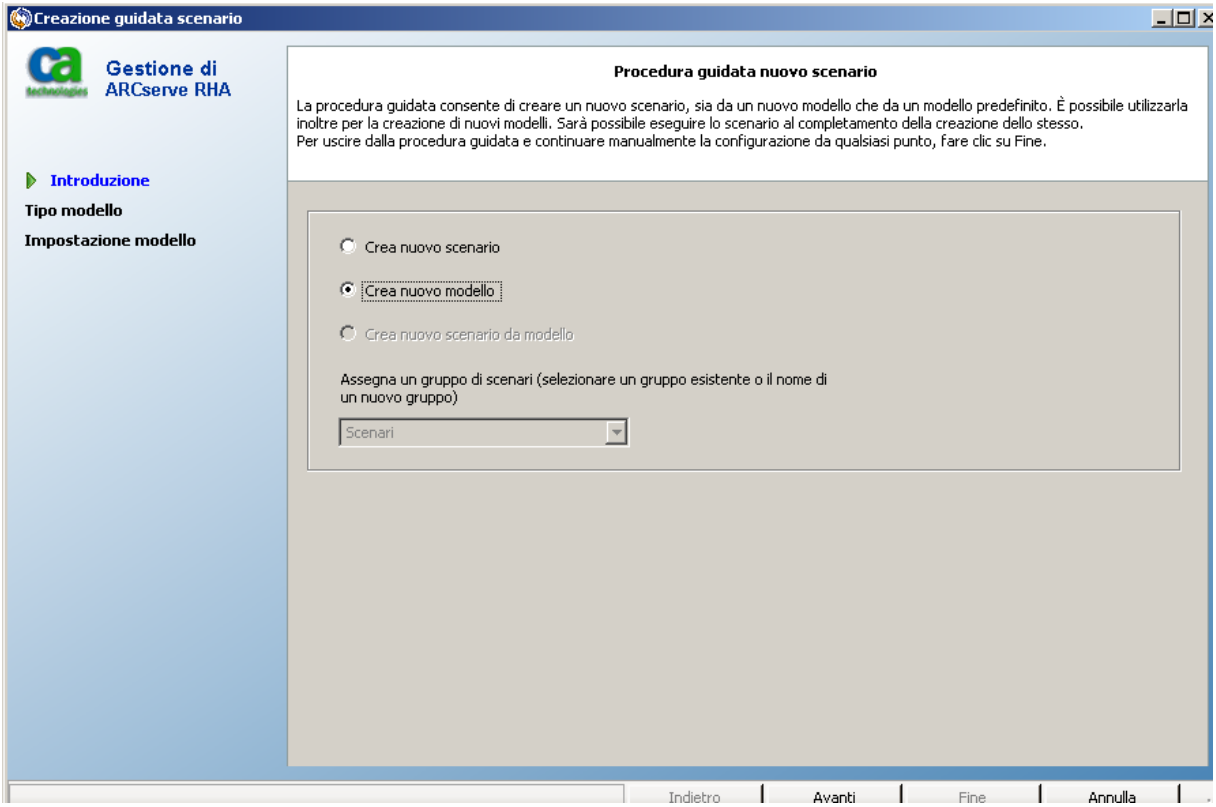
I modelli sono semplici da creare e utilizzare e il processo di creazione è di base simile a quello di un nuovo scenario. Tuttavia, poiché un modello non è associato a nessun server reale, non è possibile immettere alcuni valori quali i nomi host o gli indirizzi IP dei server master e di replica. Inoltre, sebbene sia possibile immettere i percorsi delle cartelle predefinite nella scheda Directory, occorre digitarli esplicitamente piuttosto che immetterli mediante l'esplorazione dei file.

Tutti i modelli vengono automaticamente memorizzati nella cartella **Modelli** nel riquadro Scenario. Questa cartella non viene visualizzata nel riquadro Scenario finché non viene creato almeno un modello.

Per creare un nuovo modello, procedere come segue:

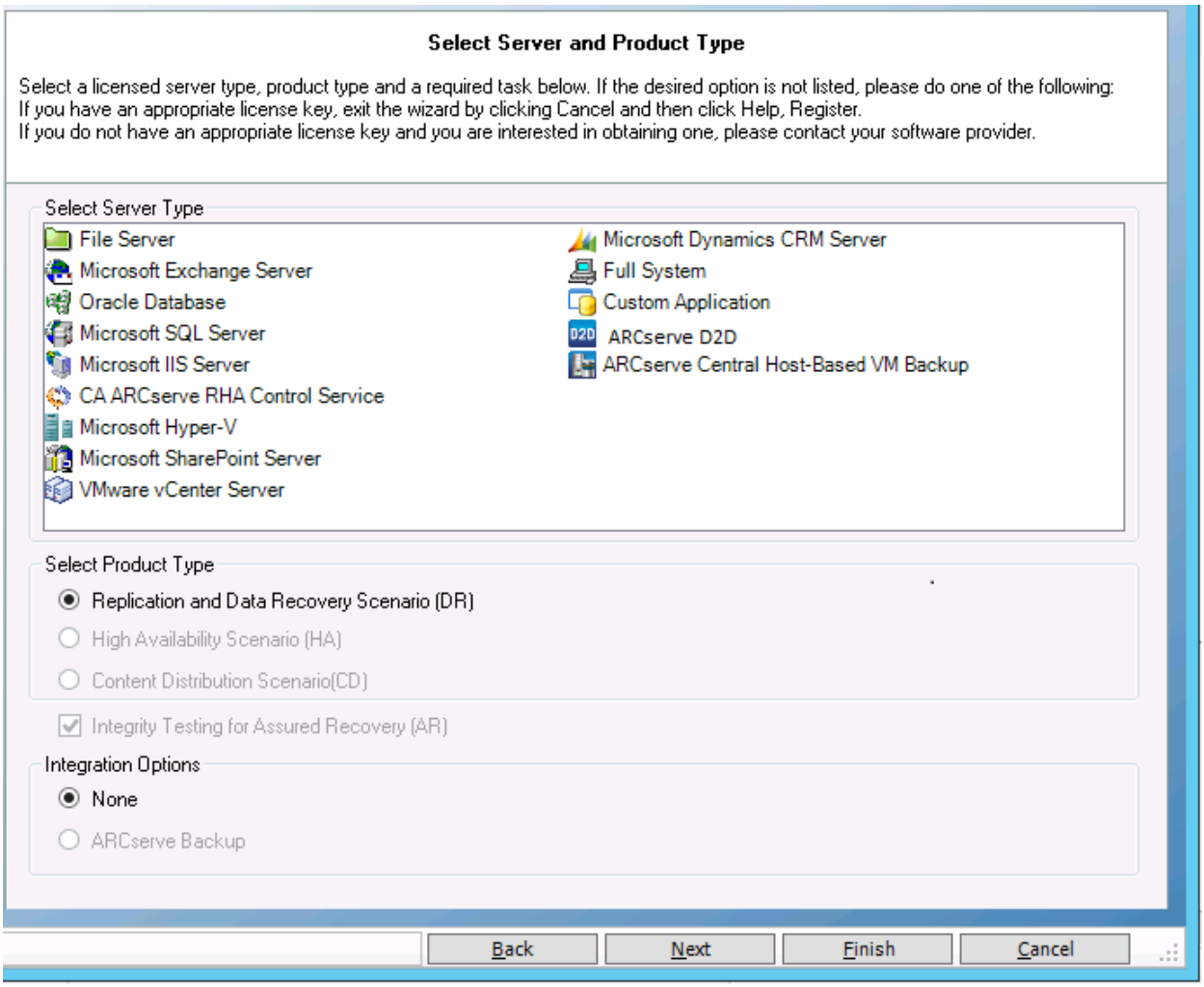
1. Aprire la creazione guidata dello scenario facendo clic sul pulsante **Nuovo** sulla barra degli strumenti standard oppure selezionando **Nuovo** dal menu **Scenario**.

   Viene visualizzata la **Creazione guidata scenario**.


Creazione guidata scenario
Gestione di ARCserve RHA
Introduzione
Tipo modello
Impostazione modello
Procedura guidata nuovo scenario
La procedura guidata consente di creare un nuovo scenario, sia da un nuovo modello che da un modello predefinito. È possibile utilizzarla inoltre per la creazione di nuovi modelli. Sarà possibile eseguire lo scenario al completamento della creazione dello stesso.
Per uscire dalla procedura guidata e continuare manualmente la configurazione da qualsiasi punto, fare clic su Fine.
Crea nuovo scenario
Crea nuovo modello
Crea nuovo scenario da modello
Assegna un gruppo di scenari (selezionare un gruppo esistente o il nome di un nuovo gruppo)
Scenari
Indietro
Avanti
Fine
Annulla

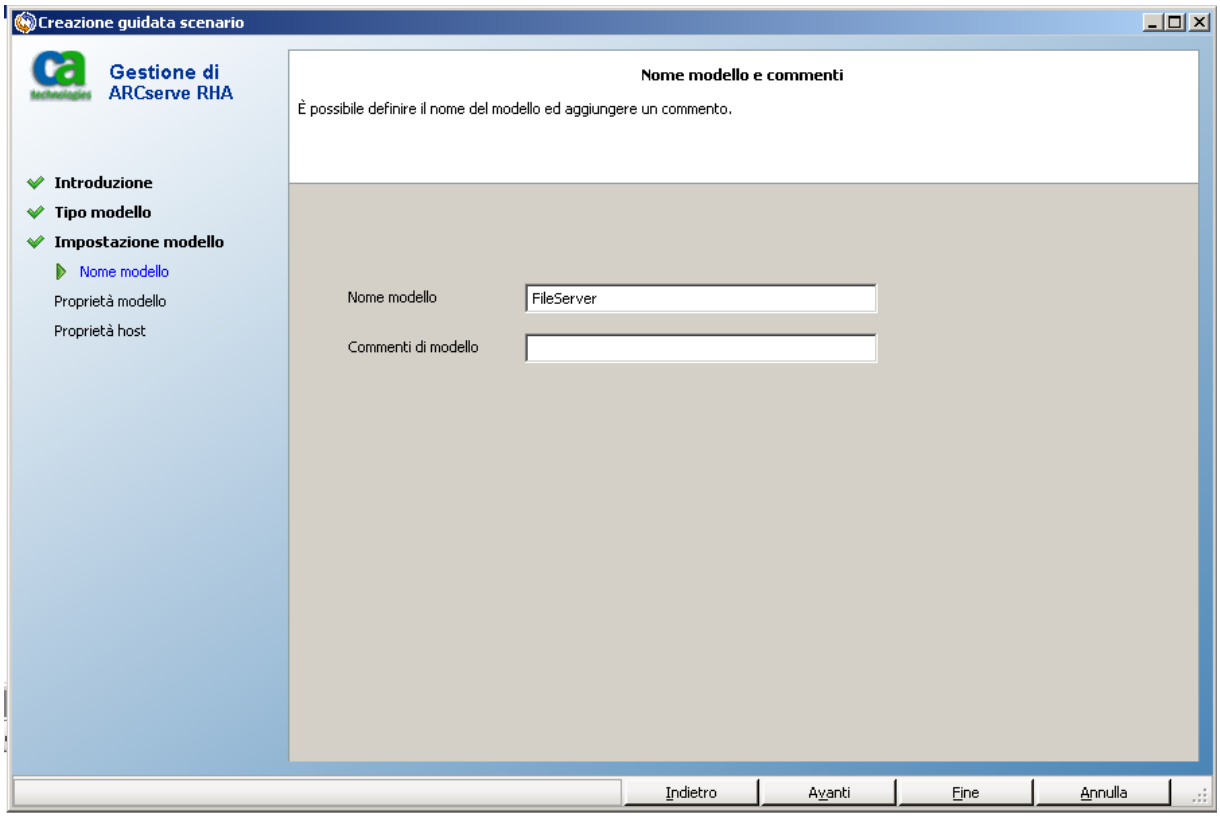
2. Selezionare il pulsante di opzione **Crea nuovo modello** e fare clic su **Avanti**.

Viene visualizzata la schermata **Selezionare server e tipo di prodotto**.


Select Server and Product Type
Select a licensed server type, product type and a required task below. If the desired option is not listed, please do one of the following:
If you have an appropriate license key, exit the wizard by clicking Cancel and then click Help, Register.
If you do not have an appropriate license key and you are interested in obtaining one, please contact your software provider.
Select Server Type
File Server
Microsoft Exchange Server
Oracle Database
Microsoft SQL Server
Microsoft IIS Server
CA ARCserve RHA Control Service
Microsoft Hyper-V
Microsoft SharePoint Server
VMware vCenter Server
Microsoft Dynamics CRM Server
Full System
Custom Application
ARCserve D2D
ARCserve Central Host-Based VM Backup
Select Product Type
Replication and Data Recovery Scenario (DR)
High Availability Scenario (HA)
Content Distribution Scenario(CD)
Integrity Testing for Assured Recovery (AR)
Integration Options
None
ARCserve Backup
Back
Next
Finish
Cancel

3. Selezionare le opzioni desiderate per lo scenario e fare clic su **Avanti**.

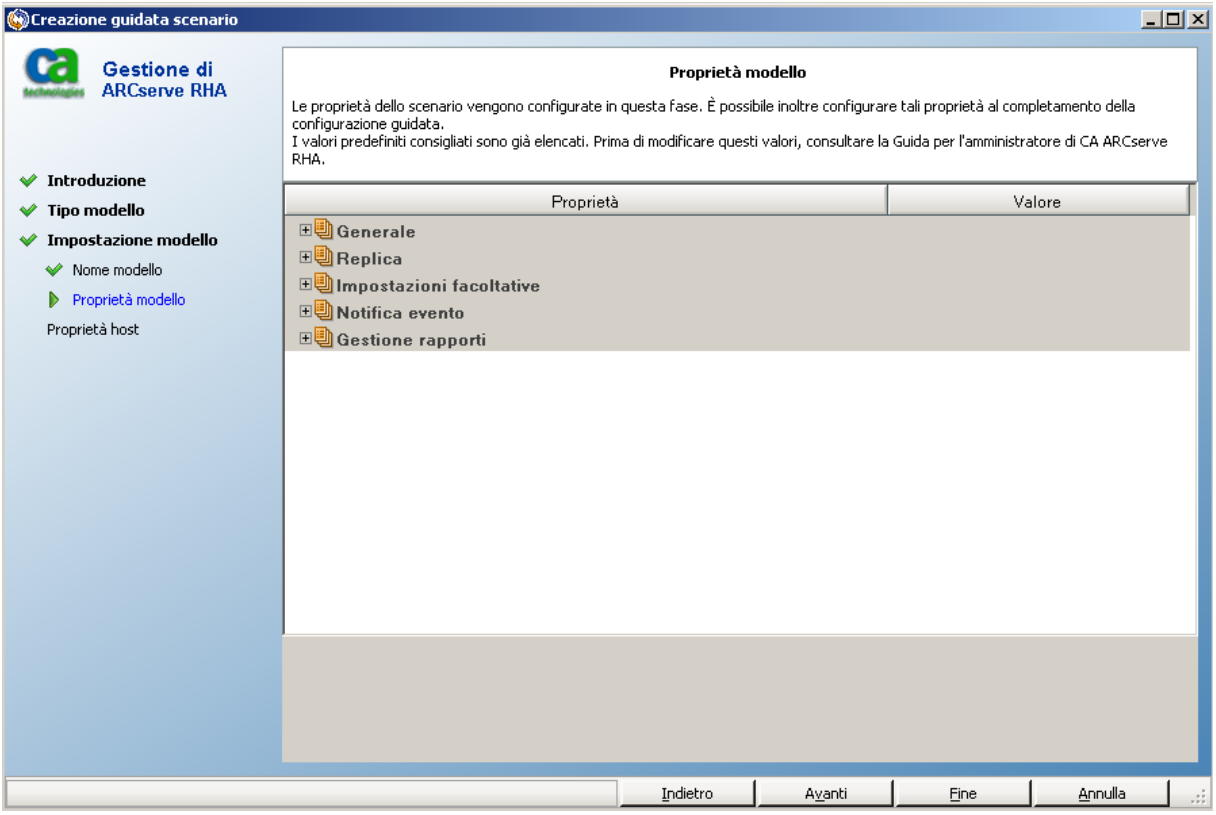
   Viene visualizzata la schermata **Nome modello e commenti**.



4. Fornire un nome e una descrizione per il modello.

   Questo nome rappresenta la base per i nomi predefiniti degli scenari che verranno creati utilizzando questo modello. Tale descrizione verrà visualizzata nel riquadro Scenario come parte dei dettagli del modello e contribuirà a identificare la configurazione del modello.

5. Fare clic su **Avanti**. Viene visualizzata la pagina **Proprietà modello**.



6. Da questo passaggio in poi, le schermate della procedura guidata sono simili a quelle relative alla creazione di un nuovo scenario (a pagina 47). Continuare a definire il modello seguendo le istruzioni della procedura guidata.

Creazione di un nuovo scenario utilizzando un modello esistente

La creazione di un nuovo scenario mediante un modello evita di dover configurare separatamente ogni scenario richiesto. Quando si utilizza uno dei modelli esistenti, viene creato un nuovo scenario con tutti i valori dei parametri ricavati da tale modello.

Nota: non è possibile creare scenari da un modello se questo non è stato salvato. La modifica dei valori dei parametri in un modello non comporterà la modifica dei valori di tali parametri in uno scenario che è stato precedentemente creato in base ad esso.

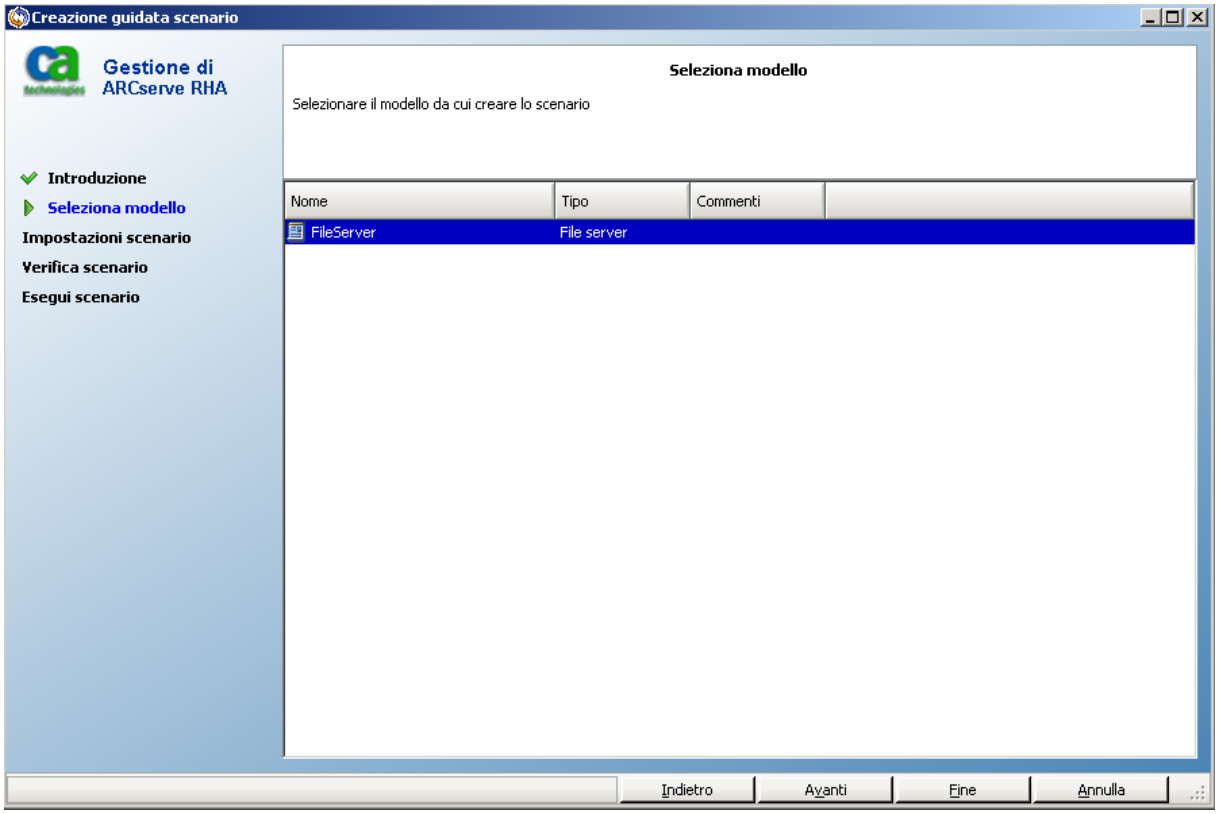
Per creare un nuovo scenario utilizzando un modello esistente

1. Aprire la creazione guidata dello scenario facendo clic sul pulsante **Nuovo** sulla barra degli strumenti standard oppure selezionando **Nuovo** dal menu **Scenario**.

   Viene visualizzata la **Creazione guidata scenario**.

2. Selezionare il pulsante opzione **Crea nuovo scenario da modello** e assegnare il nuovo scenario a un gruppo. Fare clic su **Avanti**.

   Verrà visualizzata la pagina **Seleziona modello** con un elenco di modelli disponibili.



   I modelli disponibili verranno visualizzati in questa schermata.

3. Selezionare il modello adeguato alle proprie necessità e fare clic su **Avanti**.

   Viene visualizzata la schermata **Host master e replica**.

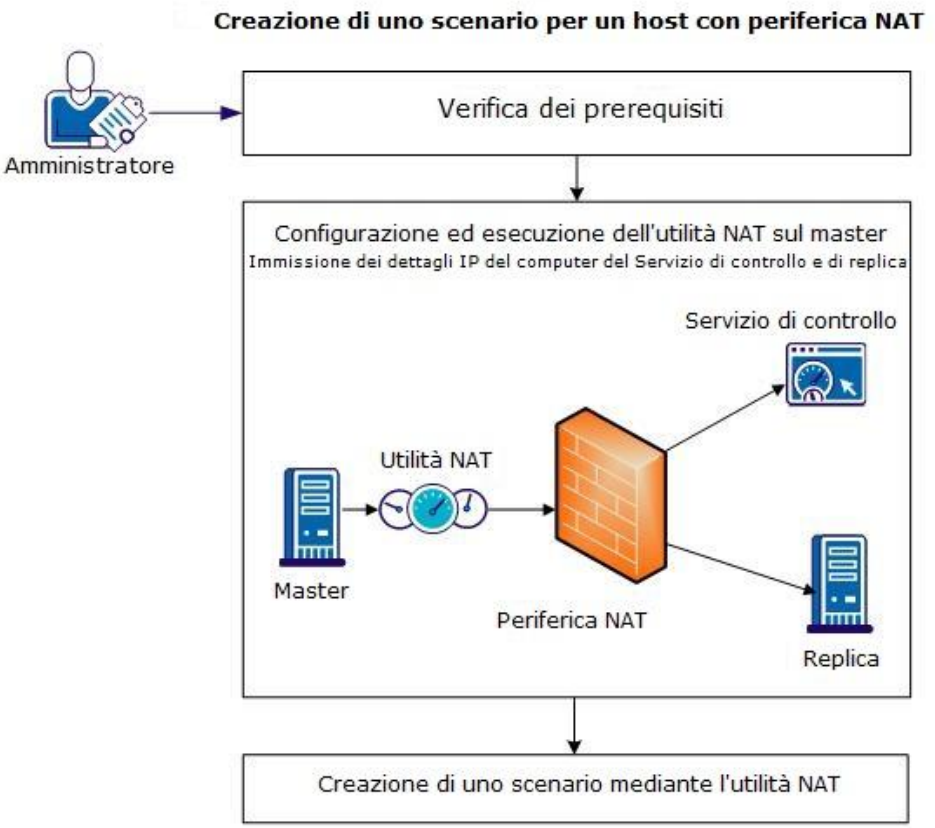
4. Il nome predefinito dello scenario è il nome del modello. È possibile lasciarlo invariato oppure modificarlo.

   Da questo passaggio in poi, le schermate della procedura guidata sono simili a quelle relative alla creazione di un nuovo scenario (a pagina 47). Procedere con la definizione del nuovo scenario seguendo le istruzioni della procedura guidata specifiche per l'applicazione che si desidera proteggere. Per ulteriori informazioni, consultare la Guida operativa appropriata.

Gestione degli host che utilizzano periferiche NAT

Il Servizio di controllo RHA consente di gestire tutte le attività associate allo scenario. Il Servizio di controllo esegue la comunicazione con i moduli RHA su tutti gli host facenti parte dello scenario. Quando l'impostazione di rete corrisponde al master o alla replica (oppure a entrambi), è necessario utilizzare una periferica NAT (Network Address Translation) per stabilire la connessione a un dominio pubblico. In tal caso, il Servizio di controllo non sarà in grado di stabilire la connessione con tali server. Per abilitare la comunicazione tra il Servizio di controllo RHA e i server, utilizzare l'utilità NAT per Arcserve RHA. È possibile configurare l'utilità NAT specificando l'indirizzo IP e i dettagli della porta del Servizio di controllo e i server del dominio pubblico.

Il seguente diagramma mostra la comunicazione tra il Servizio di controllo RHA e i server di una periferica NAT.


Creazione di uno scenario per un host con periferica NAT
Amministratore
Verifica dei prerequisiti
Configurazione ed esecuzione dell'utilità NAT sul master
Immissione dei dettagli IP del computer del Servizio di controllo e di replica
Servizio di controllo
Utilità NAT
Master
Periferica NAT
Replica
Creazione di uno scenario mediante l'utilità NAT

Per utilizzare l'utilità NAT, procedere come segue:

- Configurare l'utilità NAT (a pagina 87)
- Creare uno scenario utilizzando l'utilità NAT (a pagina 87)

Configurare l'utilità NAT

Configurare l'utilità NAT sul server master. Specificare l'indirizzo IP del Servizio di controllo e della replica per eseguire la connessione di tutti gli host e del Servizio di controllo.

Procedere come descritto di seguito:

1. Sul server master, accedere alla cartella \CA\Arcserve RHA\Engine.
2. Individuare ed eseguire il file natutlgui.exe per aprire la finestra delle impostazioni NAT.
3. Immettere l'indirizzo IP e il numero di porta del server su cui è stato installato Servizio di controllo RHA.
4. Fare clic su Aggiungi per immettere l'indirizzo IP e il numero di porta del modulo di replica.
5. Fare clic su OK per consentire all'utilità NAT di verificare la connessione al Servizio di controllo e alla replica. La visualizzazione dello stato Verificato conferma la connettività.

Nota: per utilizzare l'utilità dalla riga di comando, immettere natutl.exe.

Nota: se la replica utilizza una periferica NAT, utilizzare lo stesso processo per eseguire la configurazione dell'utilità NAT sulla replica invece che sul server master.

Creazione di uno scenario con l'utilità NAT

Dopo aver configurato e verificato la connessione dell'utilità NAT alla replica e al Servizio di controllo RHA, creare uno scenario secondo la procedura descritta nel *Capitolo 3: Creazione di scenari Replication e High Availability.*

Capitolo 4: Creazione di scenari cloud Replication e High Availability

Questa sezione contiene i seguenti argomenti:

Panoramica (a pagina 90)
Utilizzo degli scenari cloud High Availability di Arcserve RHA (a pagina 93)
Utilizzo degli scenari Arcserve RHA Replication in ambiente cloud (a pagina 94)
Pannello Visualizzazione cloud (a pagina 96)
Configurazione del proxy Web per la connessione al servizio cloud (a pagina 101)
Aggiunta di un nuovo account cloud (a pagina 102)
Modifica dell'area AWS predefinita (a pagina 104)
Aggiornamento delle informazioni dell'account cloud (a pagina 104)
Eliminazione di un account cloud (a pagina 104)
Creazione di una nuova istanza di replica EC2 (a pagina 105)
Avvio di un'istanza di replica EC2 (a pagina 111)
Interruzione di un'istanza di replica EC2 (a pagina 111)
Eliminazione di un'istanza di replica EC2 (a pagina 112)
Creazione di un nuovo scenario High Availability per sistemi completi EC2 (a pagina 112)
Creazione di un nuovo scenario di replica dei dati su EC2 (a pagina 120)
Esecuzione e sincronizzazione di uno scenario Replication o High Availability per i dati di sistemi completi EC2 (a pagina 124)
Esecuzione dell'avanzamento per uno scenario High Availability per sistemi completi EC2 (a pagina 125)
Esecuzione del recupero mediante una replica EC2 di failover (a pagina 126)

Panoramica

La versione corrente consente di eseguire la replica e di fornire l'alta disponibilità dell'applicazione negli ambienti cloud. La funzionalità di *Replication dei dati/High Availability per sistemi completi su EC2* corrisponde a un'estensione del tipo di scenario Sistema completo esistente. Questo tipo di scenario consente a Arcserve RHA di abilitare la replica e la disponibilità elevata di un sistema Windows completo sui computer virtuali in esecuzione su Microsoft Hyper-V, Citrix Xen, o VMware ESX Hypervisor. La funzionalità di *Replication dei dati/High Availability per sistemi completi su EC2* include Amazon EC2 nell'elenco degli ambienti virtuali supportati.

Per creare scenari HA per sistemi completi o scenari di replica con una replica EC2, verificare che siano soddisfatti i seguenti prerequisiti:

- È necessario disporre di un account Amazon Web Services (AWS).
- È necessario disporre di un profilo VPC configurato (Amazon Virtual Private Cloud) e creare la connessione VPN tra il server locale (dove risiede il server master) e Amazon VPC.

  Nota: per ulteriori informazioni su Amazon VPC, consultare il sito Web di Amazon.

Registrarsi su Amazon VPC
Creare un VPC
Creare una subnet
Creare un gateway cliente
Creare un gateway VPN
Connettere il gateway al VPC
Creare una connessione VPN
Configurare il gateway cliente
Avviare l'istanza EC2 sul VPC

Dopo aver verificato i requisiti, eseguire la replica e fornire la disponibilità elevata all'applicazione attenendosi alle seguenti indicazioni e utilizzando le funzionalità riportate di seguito:

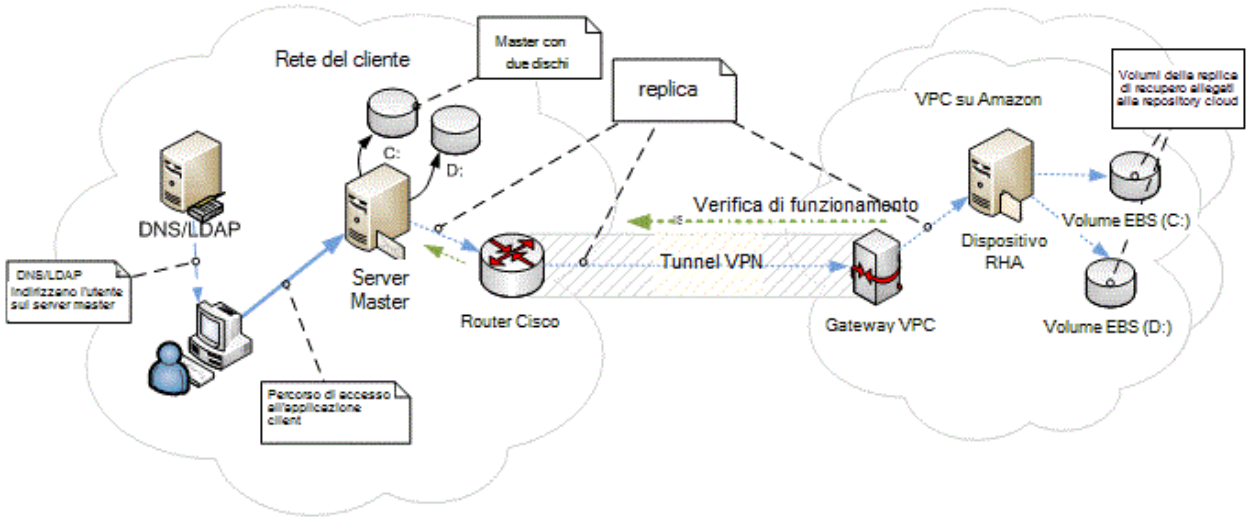
- Utilizzare l'opzione Replica su cloud di Arcserve RHA della Creazione guidata scenario.
  - Registrare l'account AWS e le credenziali in Arcserve RHA
  - Recuperare l'ID di VPC associato all'account
  - Definire l'istanza EC2 ed avviarla
  - Eseguire la distribuzione remota del Modulo Arcserve RHA
  - Utilizzare Arcserve RHA come di consueto
- Nuova scheda dell'interfaccia di Arcserve RHA per la gestione cloud (Visualizzazione cloud).
  - Mostra un elenco degli account AWS gestiti, delle istanze, snapshot, volumi EBS, indirizzi IP statici, gruppi di protezione, ecc.

Failover sistema completo EC2

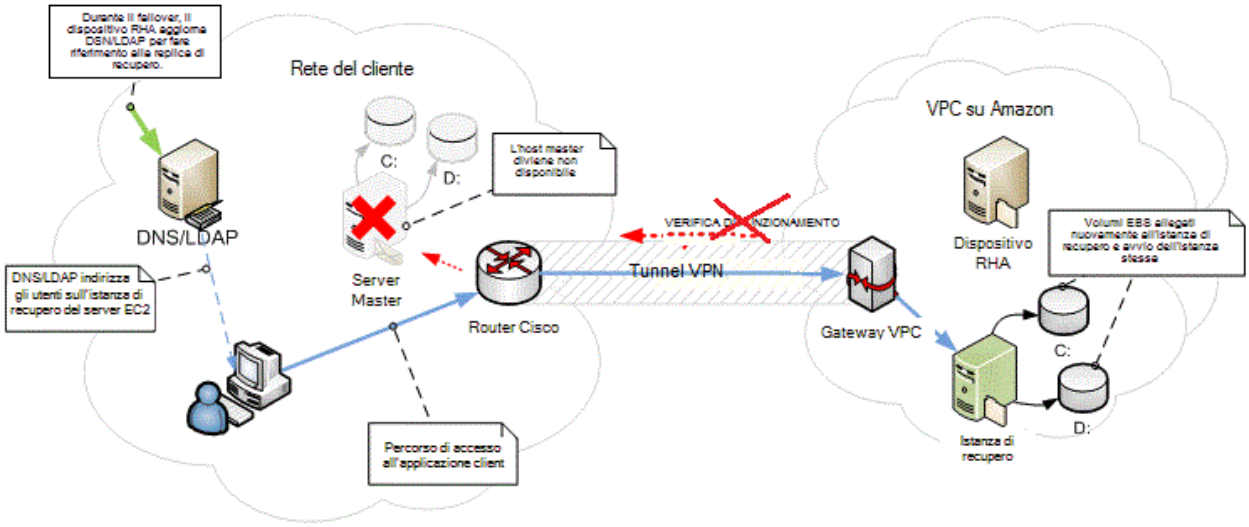
In caso di failover del sistema completo EC2, la replica avvia il processo di failover se il server master non risponde. Durante il failover vengono eseguite le seguenti azioni:

- Viene avviata una nuova istanza di recupero EC2 con la stessa versione di sistema operativo e la stessa architettura del processore utilizzata dal master, mediante un AMI predefinito e supportato. Ad esempio, se lo scenario Sistema completo EC2 protegge un server master Windows 2008 x86_64, il dispositivo Arcserve RHA esegue la nuova istanza EC2 utilizzando Windows 2008 x86_64 AMI (ami-90d420f9). Il seguente AMI pubblico verrà utilizzato con il prodotto:
  - ami-9ed420f7—istanza di recupero Windows 2003 x86_64 (us-east-1 region)
  - ami-98d420f1—istanza di recupero Windows 2003 x86 (us-east-1 region)
  - ami-ea45b883—istanza di recupero Windows 2008 R2 x86_64 (us-east-1 region)
  - ami-8bba8dff—istanza di recupero Windows 2008 R2 x86_64 (eu-west-1 region)
  - ami-61b98e15—istanza di recupero Windows 2003 x86_64 (eu-west-1 region)
  - ami-57b98e23—istanza di recupero Windows 2003 x86 (eu-west-1 region)
- Il volume di avvio EBS dell'istanza di recupero viene disconnesso dall'istanza di recupero e connesso al dispositivo Arcserve RHA.
- Le unità necessarie vengono copiate dal volume di avvio dell'istanza di recupero sul volume di avvio del master replicato, connesso al dispositivo Arcserve RHA. Inoltre, il volume master replicato viene montato e vengono create le voci di registro necessarie per abilitare le unità copiate nell'immagine Windows replicata.
- Il volume di avvio dell'istanza di recupero originale viene disconnesso dal dispositivo Arcserve RHA ed eliminato.
- I volumi EBS replicati vengono disconnessi dal dispositivo Arcserve RHA e connessi all'istanza di recupero del sistema completo EC2.
- L'istanza di recupero del sistema completo EC2 viene avviata.
- Le operazioni di failover standard restanti vengono eseguite come di consueto. Ad esempio, se abilitato, viene eseguito il reindirizzamento DNS.

L'illustrazione seguente rappresenta uno scenario di sistema completo EC2 di protezione di un server locale con due volumi EBS, prima del failover:



L'illustrazione seguente mostra gli eventi che si verificano in seguito al failover:



Utilizzo degli scenari cloud High Availability di Arcserve RHA

La funzionalità di *High Availability per sistemi completi su EC2* corrisponde a un'estensione del tipo di scenario Sistema completo esistente. Questo tipo di scenario consente a Arcserve RHA di abilitare la disponibilità elevata di un sistema Windows completo sui computer virtuali in esecuzione su Microsoft Hyper-V, Citrix Xen, o VMware ESX Hypervisor. La funzionalità di *High Availability dei dati per sistemi completi su EC2* include Amazon EC2 nell'elenco degli ambienti virtuali supportati.

La creazione di uno scenario EC2 High Availability per sistemi completi mediante la Creazione guidata scenario corrisponde alla procedura utilizzata per la creazione di uno scenario High Availability non cloud, e include le seguenti eccezioni:

- Una volta assegnato l'host master, selezionare il tipo di server *Amazon EC2* nella sezione *Impostazioni di replica* del riquadro delle assegnazioni degli host di replica e master. Selezionare l'istanza di replica EC2 (dispositivo)
- Nella schermata Proprietà di master e replica, è disponibile la nuova sezione *Cloud*. Tutte le proprietà sono di sola lettura, fatta eccezione per la proprietà *Pulizia delle risorse cloud durante la rimozione dello scenario* (disattivata per impostazione predefinita).
- Dal punto di vista della connettività, VPC viene considerato come una rete separata. Pertanto, nella schermata Proprietà avanzamento, è disponibile soltanto il metodo di reindirizzamento *Reindirizza DNS*. Per impostazione predefinita, tutti i metodi di reindirizzamento sono disabilitati, pertanto durante il failover del dispositivo di replica di EC2 viene creata un'istanza di recupero EC2 senza reindirizzamento del traffico. Se si desidera abilitare il reindirizzamento del traffico, attivare l'opzione *Reindirizza DNS*.

  Note:

  - L'opzione *Mapping di rete fisica* consente di definire la subnet VPC di avvio dell'istanza di recupero in caso di failover o avanzamento. La Creazione guidata scenario crea il mapping predefinito. Tuttavia, se lo si desidera, è possibile modificare le subnet VPC.
  - Le informazioni relative alle subnet VPC disponibili vengono recuperate da CS dal dispositivo di replica EC2 al momento della creazione dello scenario. Il dispositivo di replica EC2 stabilisce la comunicazione con il server API EC2, definito in base all'area VPC di appartenenza. I seguenti requisiti sono obbligatori:
    - Le istanze del dispositivo in esecuzione su VPC devono disporre dell'accesso a Internet (è necessario che l'amministratore di rete abiliti le regole di routing corrispondenti).
    - Le istanze dispositivo devono disporre di un set di server DNS corretto per la risoluzione degli indirizzi IP dei server API EC2.
  - Per ulteriori informazioni sulla creazione di scenari ad elevata disponibilità, consultare la sezione Creazione di scenari Replication e High Availability (a pagina 47).

Utilizzo degli scenari Arcserve RHA Replication in ambiente cloud

La funzionalità di *replica dei dati su EC2* corrisponde a un'estensione dei tipi di scenario esistenti che consentono a Arcserve RHA di abilitare la replica di un sistema Windows completo sui computer virtuali in esecuzione su Microsoft Hyper-V, Citrix Xen, o VMware ESX Hypervisor. Questa funzionalità consente di includere Amazon EC2 nell'elenco degli ambienti virtuali supportati.

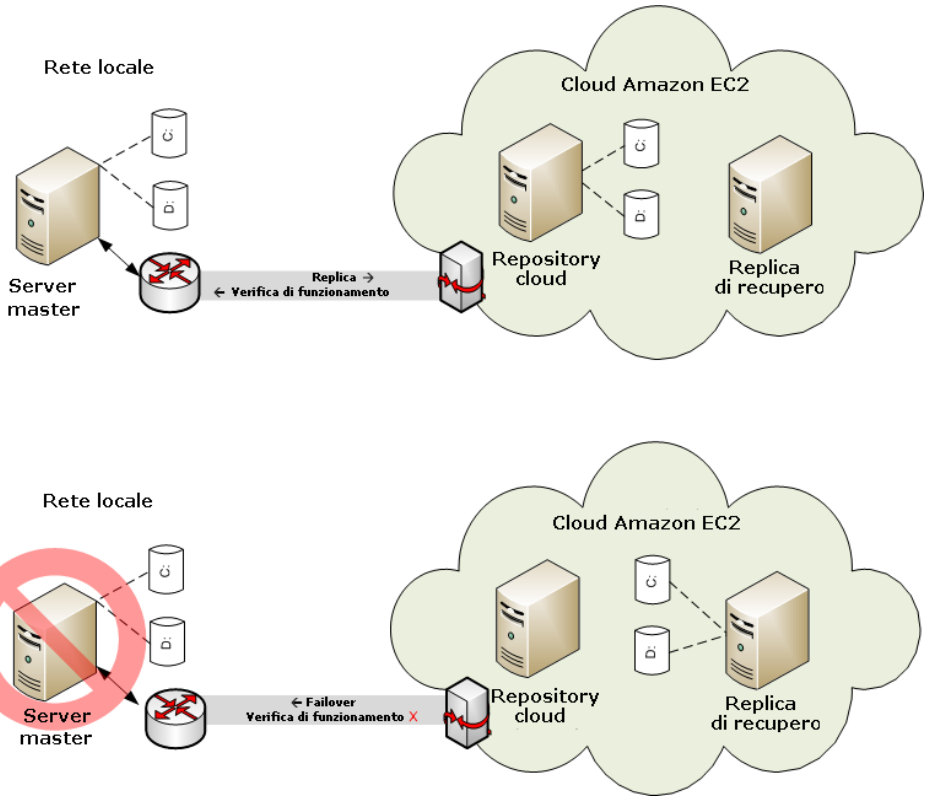
La creazione di uno scenario di replica dei dati su EC2 mediante la procedura di Creazione guidata scenario, si basa sulla procedura utilizzata per la creazione di uno scenario di replica dei dati non cloud, e include le seguenti eccezioni:

- La schermata Seleziona server e tipo prodotto, non supporta Microsoft Hyper-V per gli scenari di replica basati su cloud.
- Nella schermata Host master e replica, una volta assegnato l'host master, selezionare la casella di controllo Replica su cloud e fare clic sul pulsante Seleziona host cloud per specificare Amazon EC2 come server, quindi selezionare un'istanza di replica EC2 (dispositivo).
- Nella schermata Proprietà di master e replica, è disponibile la nuova sezione *Cloud*. Tutte le proprietà sono disponibili in sola lettura, con eccezione della proprietà *Arresta istanza quando lo scenario viene interrotto*, disabilitata per impostazione predefinita.

Nota:per ulteriori informazioni sulla creazione di scenari di replica, consultare la sezione Creazione di scenari Replication e High Availability (a pagina 47).

Replica su cloud

È ora possibile proteggere un server locale eseguendone la replica su una destinazione Amazon Web Services (AWS) basata su cloud. La Creazione guidata scenario di Arcserve RHA consente di creare e configurare un VPC e la connessione VPN tra la rete locale e la destinazione cloud.



- Il server del repository cloud corrisponde a un'istanza EC2 con Arcserve RHA.
- La replica di recupero corrisponde a un'istanza EC2 contenente lo stesso layout di disco del server master. Una volta creata, la replica di recupero viene interrotta. Viene eseguita la disconnessione di tutti i volumi che vengono quindi connessi all'istanza repository cloud. Gli scenari Arcserve RHA vengono creati dai server master locali sui volumi esposti del repository cloud.
- Se la Verifica di funzionamento non viene eseguita correttamente e viene attivato il processo di failover, i volumi esposti connessi al repository cloud vengono nuovamente connessi alla replica di recupero. La replica di recupero viene avviata. Gli utenti vengono indirizzati al server fino alla verifica della regressione.

Pannello Visualizzazione cloud

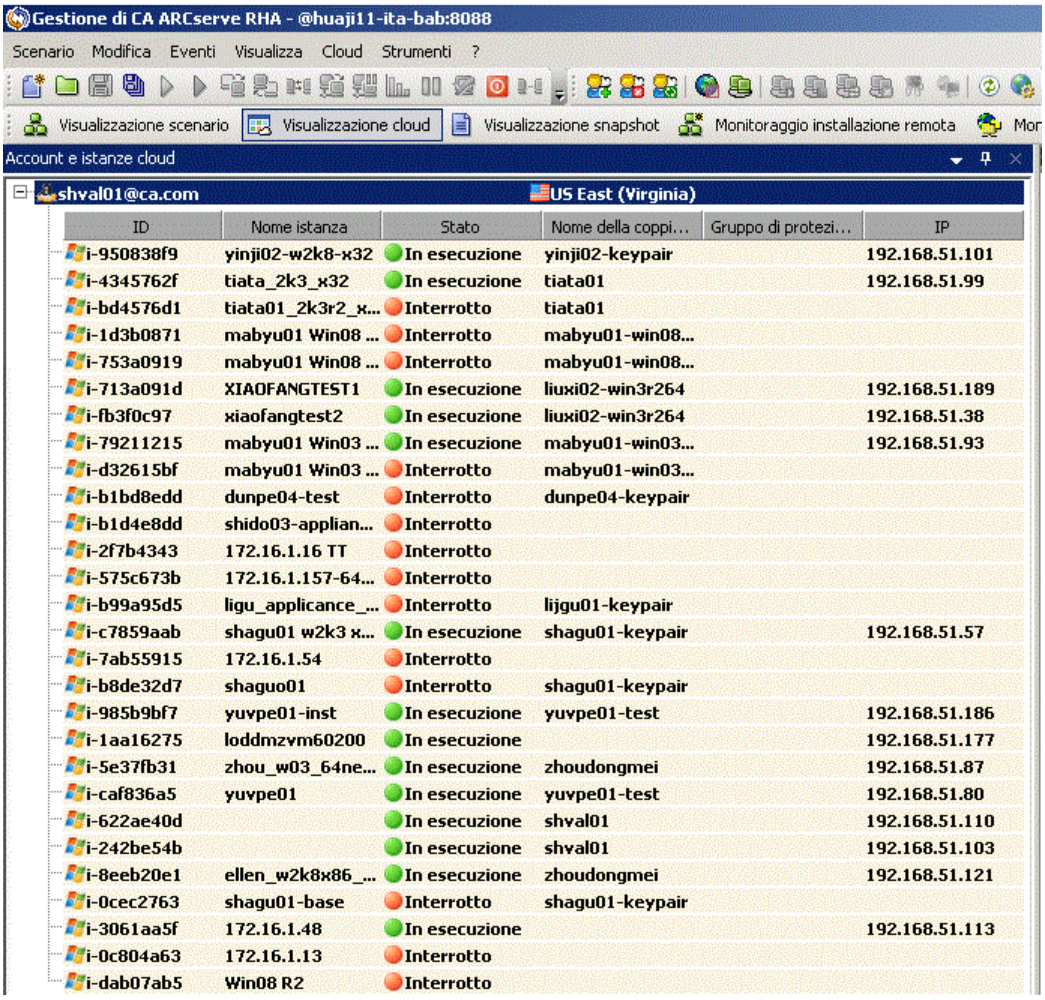
Il pannello Visualizzazione cloud consente di gestire e monitorare le istanze EC2 e supporta più account AWS.

Nota: se si desidera gestire volumi EBS snapshot, indirizzi IP statici, gruppi di protezione, ecc., utilizzare gli strumenti di gestione AWS standard, ad esempio la console di gestione di AWS.

Il pannello fornisce le seguenti opzioni:

Visualizzazione cloud

Visualizza gli account e le istanze cloud. La scheda Visualizzazione cloud contiene due riquadri. Il riquadro sinistro visualizza gli account e le istanze cloud ed include l'istanza, lo stato, il nome della coppia di chiavi, il gruppo di protezione e l'indirizzo IP.



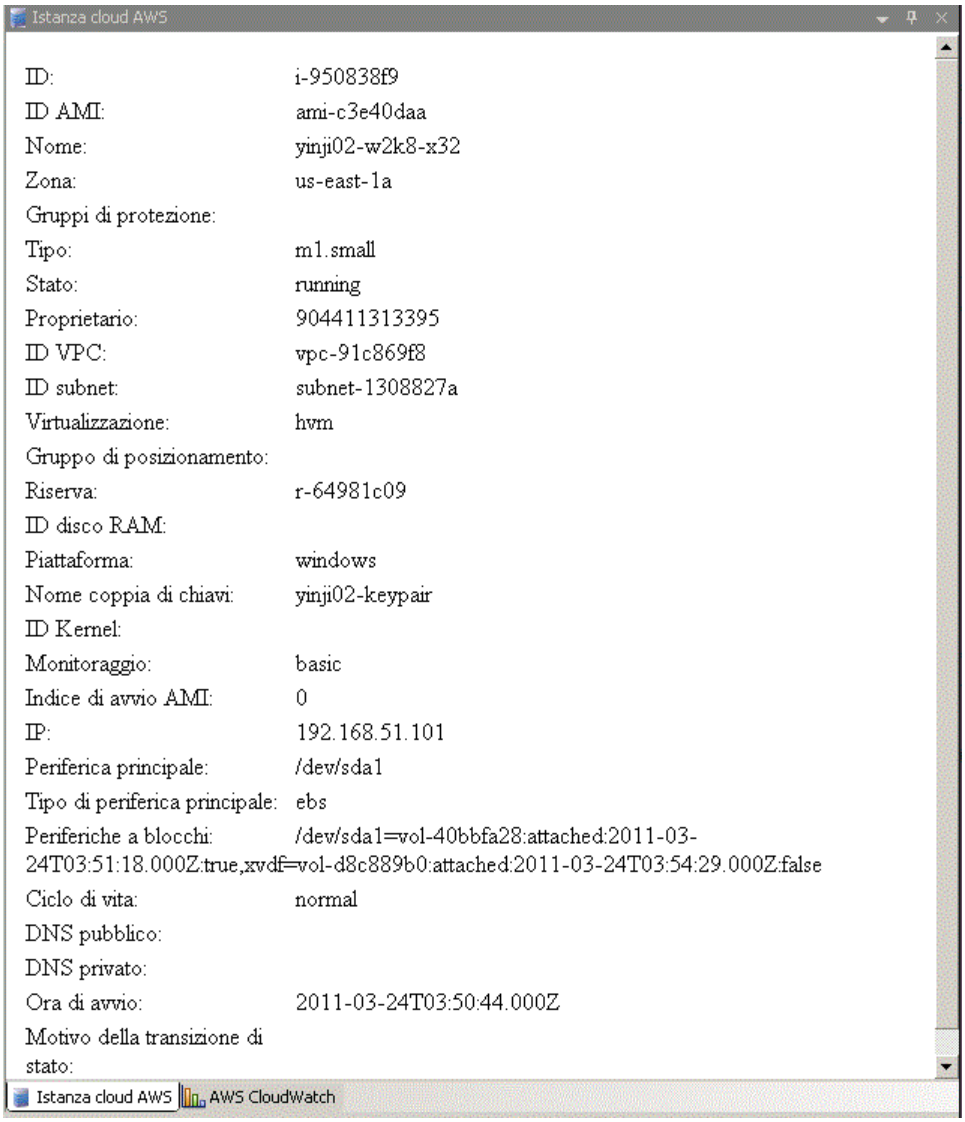
ID	Nome istanza	Stato	Nome della coppi...	Gruppo di protezi...	IP
i-950838f9	yinji02-w2k8-x32	In esecuzione	yinji02-keypair		192.168.51.101
i-4345762f	tiata_2k3_x32	In esecuzione	tiata01		192.168.51.99
i-bd4576d1	tiata01_2k3r2_x...	Interrotto	tiata01		
i-1d3b0871	mabyu01 Win08 ...	Interrotto	mabyu01-win08...		
i-753a0919	mabyu01 Win08 ...	Interrotto	mabyu01-win08...		
i-713a091d	XIAOFANGTEST1	In esecuzione	liuxi02-win3r264		192.168.51.189
i-fb3f0c97	xiaofangtest2	In esecuzione	liuxi02-win3r264		192.168.51.38
i-79211215	mabyu01 Win03 ...	In esecuzione	mabyu01-win03...		192.168.51.93
i-d32615bf	mabyu01 Win03 ...	Interrotto	mabyu01-win03...		
i-b1bd8edd	dunpe04-test	Interrotto	dunpe04-keypair		
i-b1d4e8dd	shido03-applian...	Interrotto			
i-2f7b4343	172.16.1.16 TT	Interrotto			
i-575c673b	172.16.1.157-64...	Interrotto			
i-b99a95d5	ligu_applicance_...	Interrotto	lijgu01-keypair		
i-c7859aab	shagu01 w2k3 x...	In esecuzione	shagu01-keypair		192.168.51.57
i-7ab55915	172.16.1.54	Interrotto			
i-b8de32d7	shaguo01	Interrotto	shagu01-keypair		
i-985b9bf7	yuvpe01-inst	In esecuzione	yuvpe01-test		192.168.51.186
i-1aa16275	loddmzvm60200	In esecuzione			192.168.51.177
i-5e37fb31	zhou_w03_64ne...	In esecuzione	zhoudongmei		192.168.51.87
i-caf836a5	yuvpe01	In esecuzione	yuvpe01-test		192.168.51.80
i-622ae40d		In esecuzione	shval01		192.168.51.110
i-242be54b		In esecuzione	shval01		192.168.51.103
i-8eeb20e1	ellen_w2k8x86_...	In esecuzione	zhoudongmei		192.168.51.121
i-0cec2763	shagu01-base	Interrotto	shagu01-keypair		
i-3061aa5f	172.16.1.48	In esecuzione			192.168.51.113
i-0c804a63	172.16.1.13	Interrotto			
i-dab07ab5	Win08 R2	Interrotto			

Account cloud AWS

Visualizza il pannello delle statistiche AWS contenente il riepilogo di utilizzo delle risorse EC2 per l'account Cloud. Questo riquadro viene visualizzato nella parte destra, quando una voce dell'account AWS viene selezionata nel riquadro sinistro.

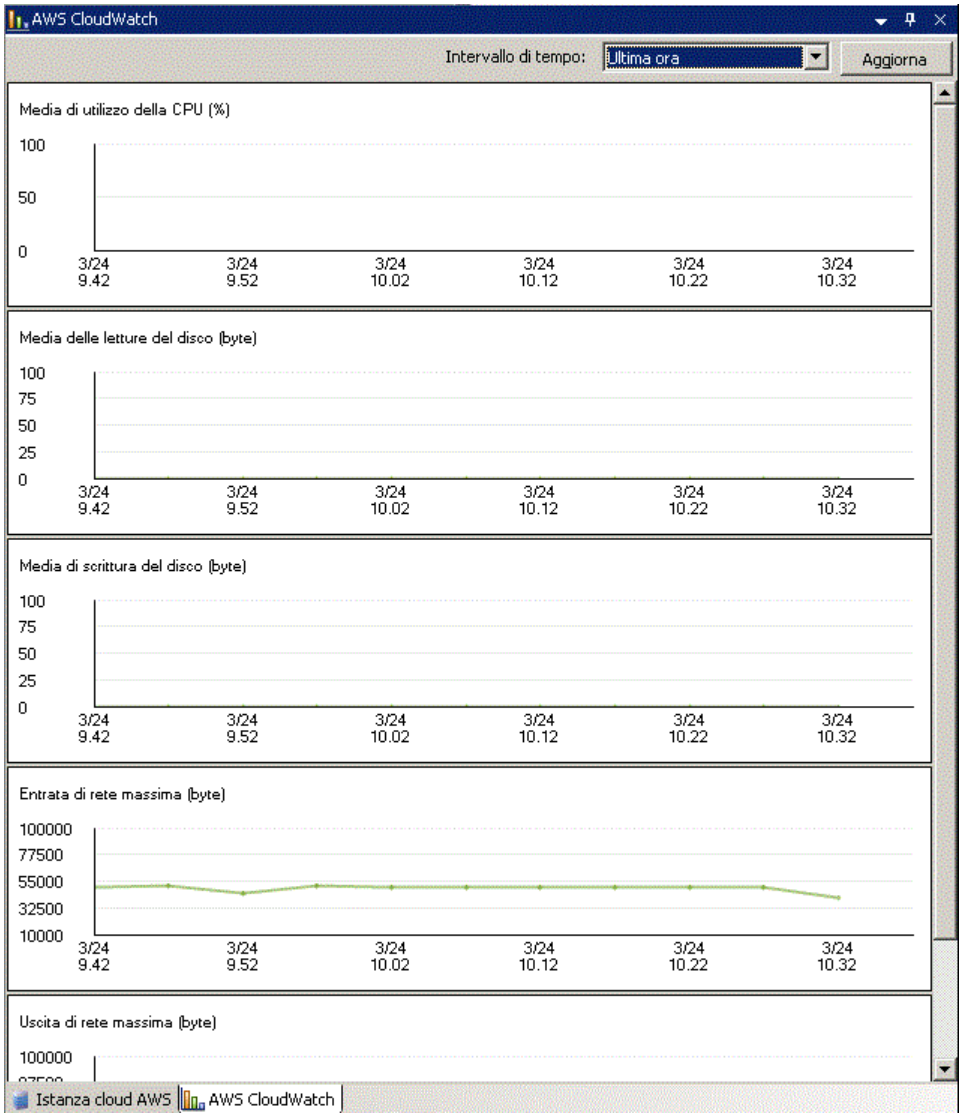
Istanza cloud AWS

Visualizza il pannello delle statistiche AWS contenente le informazioni dettagliate relative all'istanza. Questo riquadro viene visualizzato nella parte destra, quando viene selezionata un'istanza specifica nel riquadro sinistro.



AWS CloudWatch

Se abilitata, visualizza statistiche di istanza aggiuntive.



Quando il riquadro Visualizzazione cloud viene utilizzato, la barra degli strumenti corrispondente viene attivata. Utilizzare le seguenti opzioni della barra degli strumenti Visualizzazione cloud per la gestione di account e istanze cloud:

Aggiungi account cloud

Apre la finestra di dialogo Aggiungi account cloud per la creazione di un nuovo account cloud.

Elimina account cloud

Consente di eliminare l'account cloud selezionato.

Aggiorna account cloud

Consente di modificare le informazioni dell'account cloud.

Modifica area predefinita

Consente di modificare l'area AWS predefinita.

Crea nuova istanza

Consente di accedere alla Procedura guidata di creazione istanza e creare una nuova istanza.

Elimina istanza

Consente di eliminare l'istanza selezionata.

Avvia istanza

Consente di avviare l'istanza selezionata.

Interrompi istanza

Consente di interrompere l'istanza selezionata.

Riavvia istanza

Consente di riavviare l'istanza interrotta.

Acquisisci password

Consente di recuperare la password di un'istanza.

Aggiorna

Consente di aggiornare l'account e le istanze cloud visualizzate nella Visualizzazione cloud.

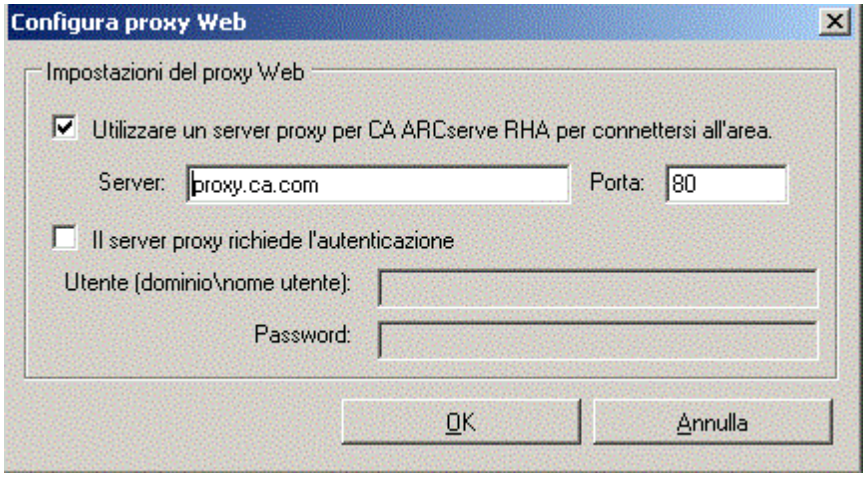
Configure Web Proxy Server (Configura server proxy Web)

Consente di specificare le informazioni relative al proxy, quali indirizzo IP, porta e credenziali utente per la connessione al servizio cloud.

Configurazione del proxy Web per la connessione al servizio cloud

Se si desidera utilizzare l'opzione *Utilizzare il proxy per la connessione al servizio cloud* della finestra di dialogo Aggiungi account cloud, è necessario configurare il proxy Web che si desidera utilizzare per la gestione delle risorse EC2.

Per configurare il proxy Web, fare clic sul pulsante Configurazione proxy Web della barra degli strumenti del riquadro Visualizzazione cloud e immettere le informazioni di impostazione del proxy Web (ad esempio, server, porta e credenziali utente). Viene inviata al server una richiesta di verifica delle impostazioni del proxy. Una volta completata la verifica, le impostazioni del proxy vengono salvate nell'account AWS.



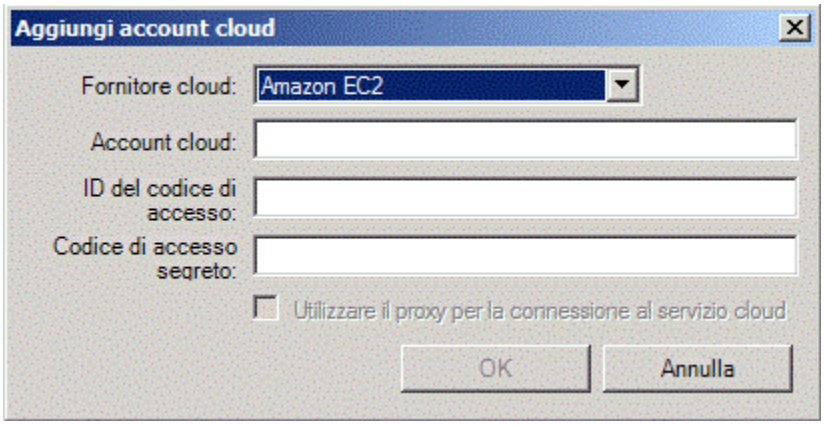
Aggiunta di un nuovo account cloud

Per visualizzare e gestire le istanze EC2 nel riquadro Visualizzazione cloud, aggiungere un nuovo account cloud utilizzando le credenziali AWS.

Per aggiungere un nuovo account cloud

1. Fare clic sul pulsante Aggiungi account cloud della barra degli strumenti.

   Viene visualizzata la finestra di dialogo Aggiungi account cloud.



2. Immettere le informazioni necessarie nei seguenti campi:

   Fornitore cloud

   Specifica il nome del servizio del fornitore cloud.

   Account cloud

   Specifica l'account cloud. In genere si tratta dell'indirizzo di posta elettronica utilizzato per registrare l'account AWS.

   ID del codice di accesso

   Specifica l'ID del codice di accesso per l'account AWS.

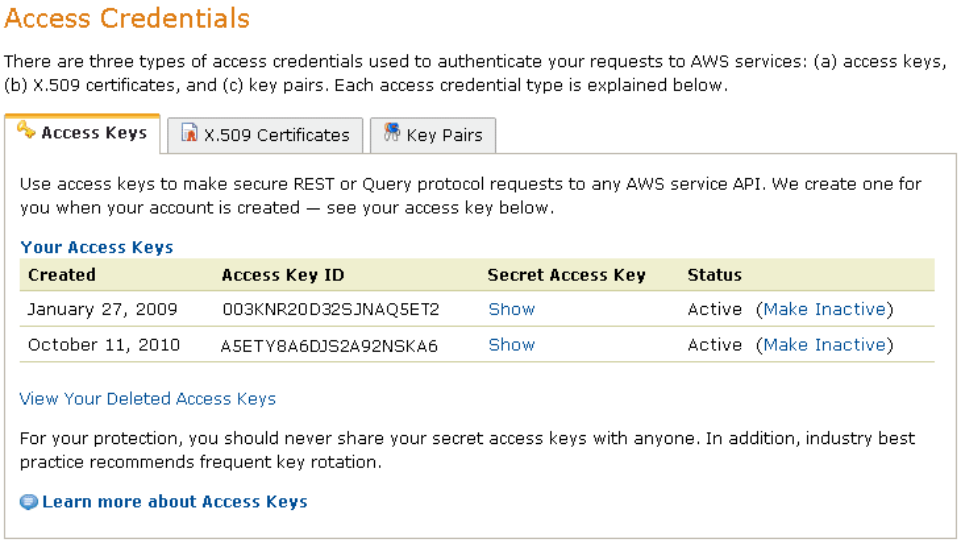
   Codice di accesso segreto

   Consente di immettere il codice di accesso segreto fornito dall'account AWS.

   (Facoltativo) Utilizzare il proxy per la connessione al servizio cloud

   Consente di specificare se utilizzare un proxy Web per comunicare con il server dei servizi Web AWS. Se si seleziona questa casella di controllo per attivare l'opzione, verificare che il proxy sia stato configurato (a pagina 101).

   Nota: le informazioni richieste per questi campi sono disponibili nella pagina principale dell'account AWS, nella scheda contenente le credenziali di protezione.


Access Credentials
There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.
Access Keys
X.509 Certificates
Key Pairs
Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.
Your Access Keys
Created
Access Key ID
Secret Access Key
Status
January 27, 2009
003KNR20D32SJNAQ5ET2
Show
Active (Make Inactive)
October 11, 2010
A5ETY8A6DJS2A92NSKA6
Show
Active (Make Inactive)
View Your Deleted Access Keys
For your protection, you should never share your secret access keys with anyone. In addition, industry best practice recommends frequent key rotation.
Learn more about Access Keys

3. Fare clic su OK (Salva/Applica).

   La finestra di dialogo Aggiungi account cloud viene chiusa. L'account cloud viene visualizzato nel riquadro Visualizzazione cloud come account cloud registrato e visualizza tutte le istanze EC2 appartenenti a tale account.

Modifica dell'area AWS predefinita

Nel riquadro Visualizzazione cloud, è possibile selezionare un'area AWS diversa durante la gestione delle istanze EC2. Per modificare l'area AWS predefinita, fare clic sul pulsante Modifica area predefinita della barra degli strumenti. Nella finestra di dialogo Modifica area predefinita, selezionare un'area diversa dall'elenco a discesa. Il pannello Visualizzazione cloud viene aggiornato con le istanze disponibili per l'area selezionata.

Aggiornamento delle informazioni dell'account cloud

È possibile aggiornare le credenziali di un account cloud configurato precedentemente. Ad esempio, se l'ID del codice di accesso e il Codice di accesso segreto sono stati modificati utilizzando la console di gestione di Amazon (mediante la generazione di una nuova coppia e la disattivazione della coppia di precedente), è necessario aggiornare manualmente le credenziali dell'account AWS. Per aggiornare le informazioni relative alle credenziali dell'account cloud, selezionare nel riquadro Visualizzazione cloud l'account cloud che si desidera aggiornare, quindi fare clic sul pulsante Aggiorna account cloud della barra degli strumenti. Immettere le nuove credenziali e fare clic su OK. Le informazioni relative all'account cloud vengono aggiornate nel riquadro Visualizzazione cloud.

Eliminazione di un account cloud

È possibile eliminare gli account cloud non utilizzati. Per eliminare un account cloud, selezionare nel riquadro Visualizzazione cloud l'account cloud che si desidera eliminare, quindi fare clic sul pulsante Elimina account cloud della barra degli strumenti. L'account cloud viene eliminato dall'elenco del riquadro Visualizzazione cloud.

Creazione di una nuova istanza di replica EC2

Per utilizzare le funzionalità cloud di Arcserve RHA negli scenari Replication o High Availability per sistemi completi, è necessario creare un'istanza di replica EC2. Verificare i seguenti requisiti prima di avviare questa procedura:

- L'account Amazon Web Services (AWS) è stato creato
- L'Amazon Virtual Private Cloud (VPC) è stato creato e connesso alla rete locale mediante VPN

  Nota: per ulteriori informazioni su Amazon VPC, consultare il sito Web di Amazon.
- L'account AWS è stato registrato nella Gestione Arcserve RHA

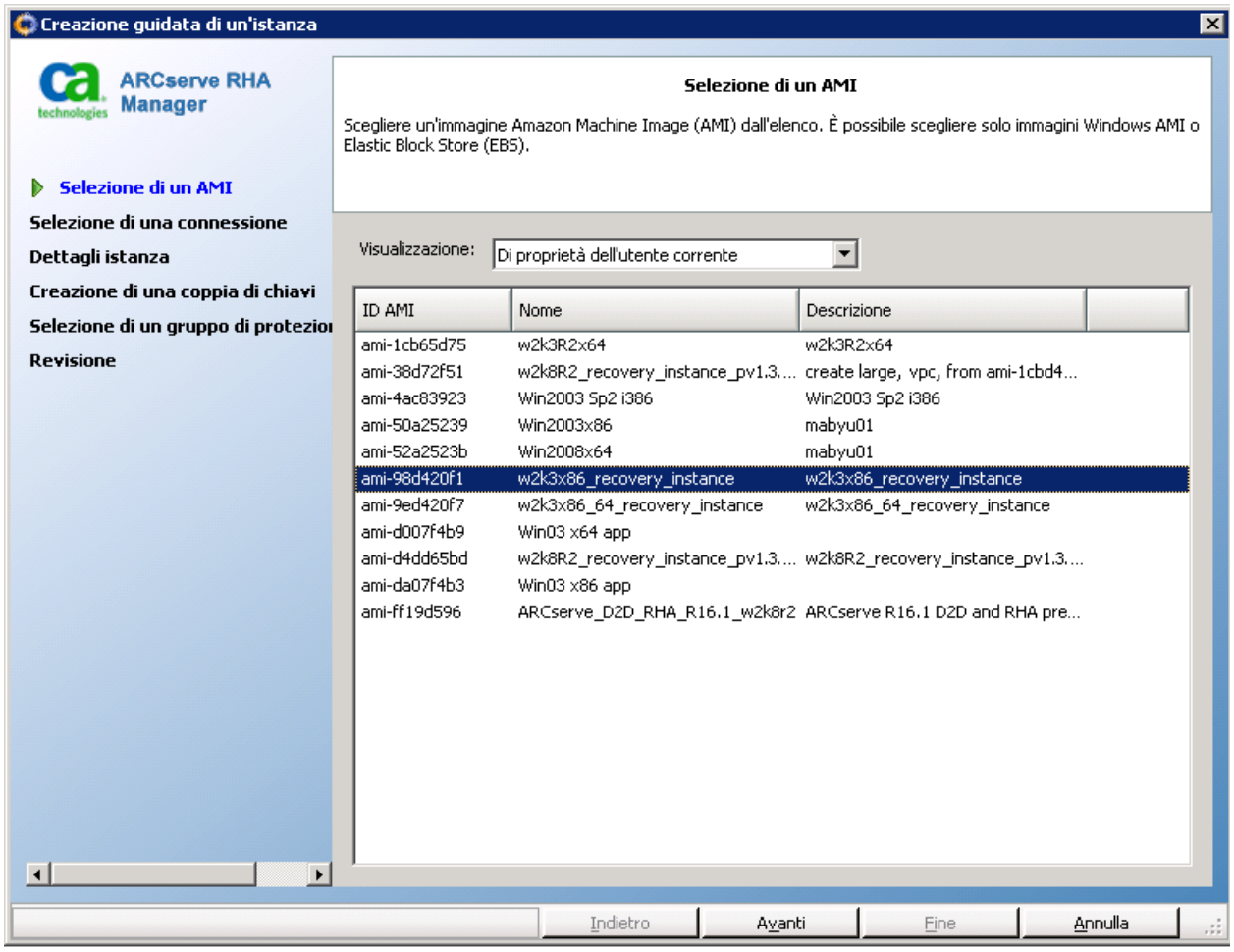
Nota: per ulteriori informazioni su EC2, inclusi i dettagli relativi all'istanza e alla creazione delle coppie di chiavi (richieste per questa procedura) consultare la documentazione Amazon EC2 disponibile sul sito Web Amazon.

Per creare una nuova istanza di replica EC2

1. Selezionare il riquadro Visualizzazione cloud nella Gestione Arcserve RHA.

   Le istanze create precedentemente vengono visualizzate nell'elenco Account e istanze cloud dell'area specificata. Per specificare un'area predefinita diversa, fare clic sul pulsante Modifica area predefinita della barra degli strumenti.
2. Fare clic con il pulsante destro sull'account AWS che si desidera utilizzare, quindi selezionare Crea istanza.

   Viene visualizzata la Creazione guidata dell'istanza.



3. Selezionare un'immagine Amazon Machine Image (AMI) dall'elenco della finestra di dialogo Selezionare un AMI, quindi fare clic su Avanti.

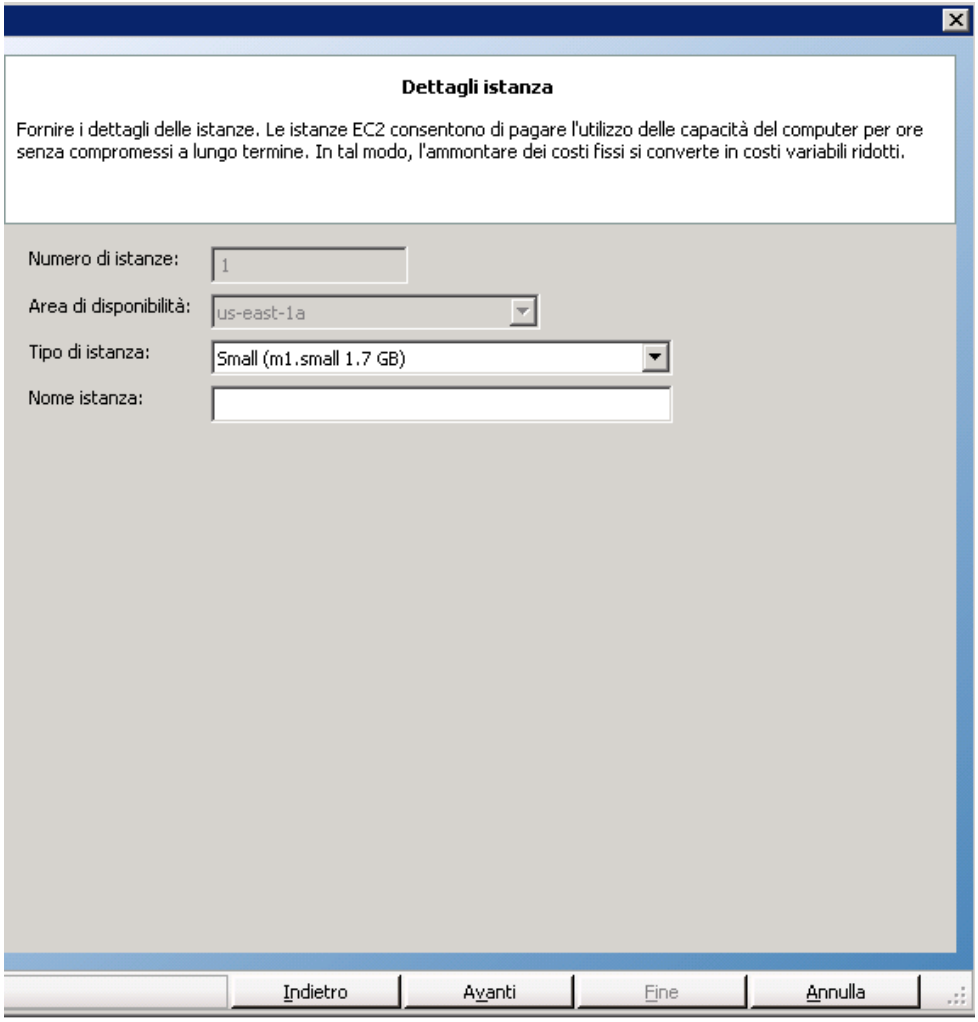
   Nota: è possibile utilizzare solo AMI di Windows con backup EBS.

   Viene visualizzata la schermata Seleziona connessione.

4. Specificare la subnet VPC per l'allocazione dell'istanza e fare clic su Avanti.

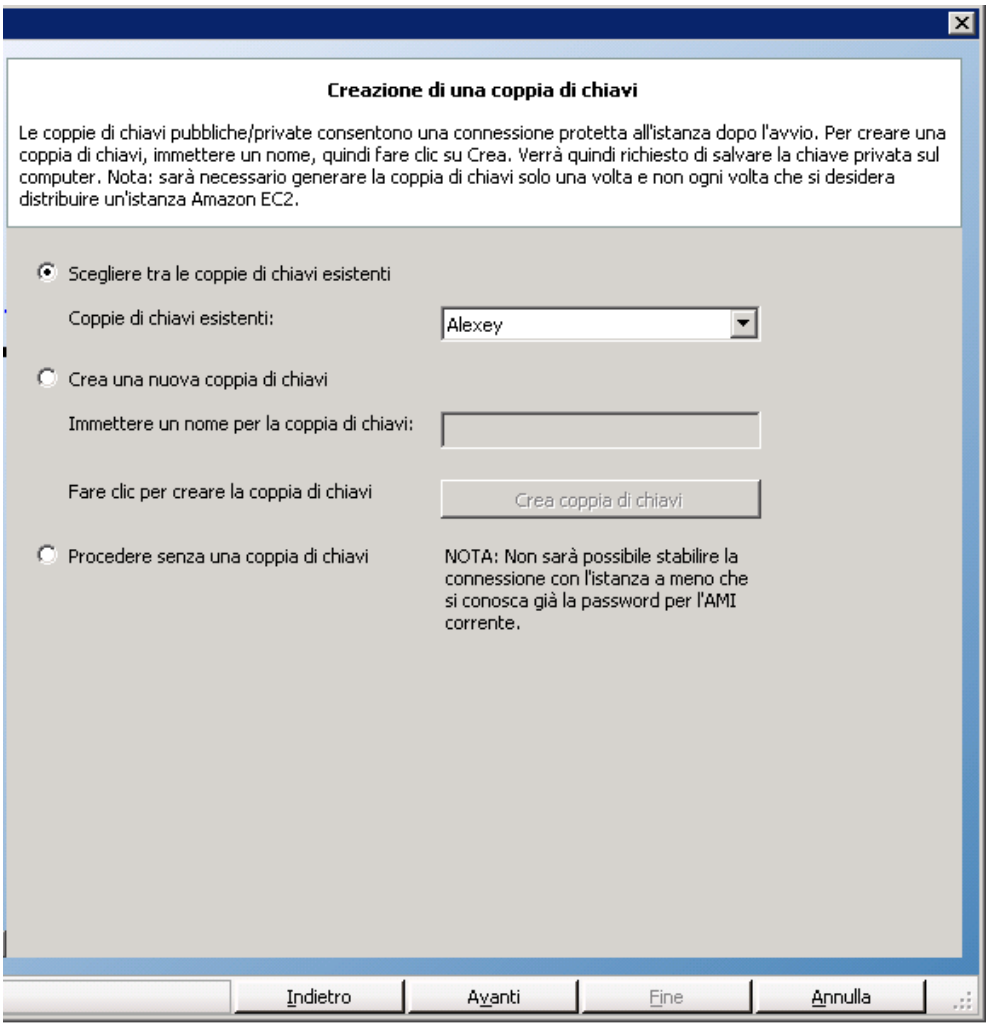
   Nota: un indirizzo DHCP viene assegnato automaticamente all'istanza dall'intervallo IP della subnet utilizzata per l'allocazione.

   Viene visualizzata la schermata Dettagli istanza.


Dettagli istanza
Fornire i dettagli delle istanze. Le istanze EC2 consentono di pagare l'utilizzo delle capacità del computer per ore senza compromessi a lungo termine. In tal modo, l'ammontare dei costi fissi si converte in costi variabili ridotti.
Numero di istanze:
1
Area di disponibilità:
us-east-1a
Tipo di istanza:
Small (m1.small 1.7 GB)
Nome istanza:
Indietro
Avanti
Fine
Annulla

5. Specificare il numero di istanze, l'area di disponibilità e il tipo di istanza, quindi fare clic su Avanti. Le istanze consentono di eseguire la fatturazione per ore dell'utilizzo delle capacità del computer senza compromessi a lungo termine. In tal modo, l'ammontare dei costi fissi si converte in costi variabili ridotti.

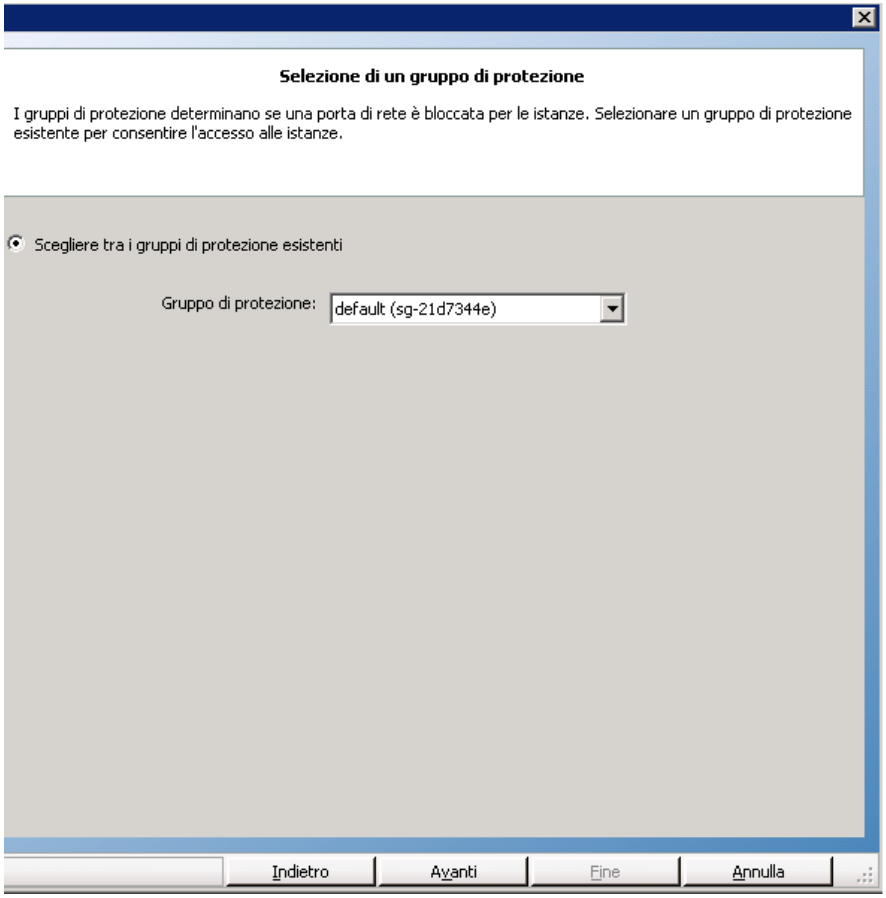
   Viene visualizzata la schermata Crea coppia di chiavi.


Creazione di una coppia di chiavi
Le coppie di chiavi pubbliche/private consentono una connessione protetta all'istanza dopo l'avvio. Per creare una coppia di chiavi, immettere un nome, quindi fare clic su Crea. Verrà quindi richiesto di salvare la chiave privata sul computer. Nota: sarà necessario generare la coppia di chiavi solo una volta e non ogni volta che si desidera distribuire un'istanza Amazon EC2.
Scegliere tra le coppie di chiavi esistenti
Coppie di chiavi esistenti:
Alexey
Crea una nuova coppia di chiavi
Immettere un nome per la coppia di chiavi:
Fare clic per creare la coppia di chiavi
Crea coppia di chiavi
Procedere senza una coppia di chiavi
NOTA: Non sarà possibile stabilire la connessione con l'istanza a meno che si conosca già la password per l'AMI corrente.
Indietro
Avanti
Fine
Annulla

6. Selezionare una coppia di chiavi esistente o creare una nuova coppia di chiavi per la connessione protetta all'istanza, in seguito all'avvio. Nel caso in cui venga creata una nuova coppia di chiavi, è necessario salvare la chiave privata sul computer. Fare clic su Avanti.

   Nota: è sufficiente generare la coppia di chiavi una sola volta, e non ogni volta che si desidera eseguire la distribuzione di un'istanza.

   Viene visualizzata la schermata Selezione di un gruppo di protezione.


Selezione di un gruppo di protezione
I gruppi di protezione determinano se una porta di rete è bloccata per le istanze. Selezionare un gruppo di protezione esistente per consentire l'accesso alle istanze.
Scegliere tra i gruppi di protezione esistenti
Gruppo di protezione:
default (sg-21d7344e)
Indietro
Avanti
Fine
Annulla

7. Selezionare un gruppo di protezione e fare clic su Avanti.

   Nell'elenco sono riportati i gruppi di protezione esistenti.

   Viene visualizzata la schermata Revisione.

8. Verificare le informazioni specificate e fare clic su Fine.

   L'istanza viene creata e la password predefinita viene inviata all'utente.

   Note:

   - Il riquadro Visualizzazione cloud consente solo la creazione di istanze basate su computer virtuale. Poiché non è possibile allocare un'istanza all'esterno del computer virtuale, la configurazione del computer virtuale è obbligatoria.
   - È possibile creare istanze non-VPC (istanze pubbliche) utilizzando gli strumenti di gestione AWS (nella console di gestione di AWS). Le istanze pubbliche vengono visualizzate nel riquadro Visualizzazione cloud. Tuttavia, tali istanze non saranno disponibili nella Creazione guidata scenario, in quanto la procedura guidata supporta solo scenari di tipo privato-privato e la replica da una rete locale privata su computer virtuale
   - È possibile applicare un filtro alla ricerca di risorse, selezionando aree diverse. Gli utenti AWS dispongono di sette aree: Europa occidentale (Irlanda), est degli Stati Uniti (Virginia), ovest degli Stati Uniti (Nord California), ovest degli Stati Uniti (Oregon), America del Sud (São Paulo), Asia-Pacifico (Tokyo), Asia-Pacifico (Singapore). Attualmente, AWS consente la creazione di un solo computer virtuale per AWS. Ciascun computer virtuale può disporre di più subnet. L'ID della subnet viene selezionato in seguito all'allocazione dell'istanza. La subnet può trovarsi in una delle quattro aree indicate. Se si desidera allocare un'istanza in una subnet specifica, selezionare prima l'area corrispondente nel menu a discesa *Modifica area predefinita*. Tuttavia, considerare che RHA supporta unicamente cinque aree: est degli Stati Uniti (Virginia), Europa occidentale (Irlanda), Asia Pacifico (Tokyo), Asia Pacifico (Sidney) e America del Sud (Sao Paulo).

Avvio di un'istanza di replica EC2

Per avviare un'istanza EC2 interrotta nel riquadro Visualizzazione cloud, selezionare l'istanza EC2 che si desidera avviare e fare clic sul pulsante Avvia istanza della barra degli strumenti. Lo stato dell'istanza EC2 selezionata nel riquadro Visualizzazione cloud viene modificato da *Interrotto* a *In attesa di esecuzione*, e infine a *In esecuzione*.

Interruzione di un'istanza di replica EC2

Per interrompere, senza rimuovere, un'istanza EC2 non utilizzata dal riquadro Visualizzazione cloud, selezionare l'istanza EC2 che si desidera interrompere e fare clic sul pulsante Interrompi istanza della barra degli strumenti. Lo stato dell'istanza EC2 selezionata nel riquadro Visualizzazione cloud viene modificato da *In esecuzione* a *Interrotto*.

Eliminazione di un'istanza di replica EC2

Per eliminare un'istanza EC2 non utilizzata dal riquadro Visualizzazione cloud, selezionare l'istanza EC2 che si desidera eliminare e fare clic sul pulsante Elimina istanza della barra degli strumenti. L'istanza EC2 viene rimossa dall'elenco delle istanze del riquadro Visualizzazione cloud.

Creazione di un nuovo scenario High Availability per sistemi completi EC2

È possibile creare uno scenario High Availability per sistemi completi EC2 ed eseguire la replica di un sistema Windows locale completo su un AMI Windows con backup EBS che verrà portata in linea in caso di errore del server master. Tale procedura avvia la creazione guidata degli scenari High Availability, che guida l'utente attraverso i vari passaggi necessari. È possibile configurare le proprietà senza utilizzare la procedura guidata.

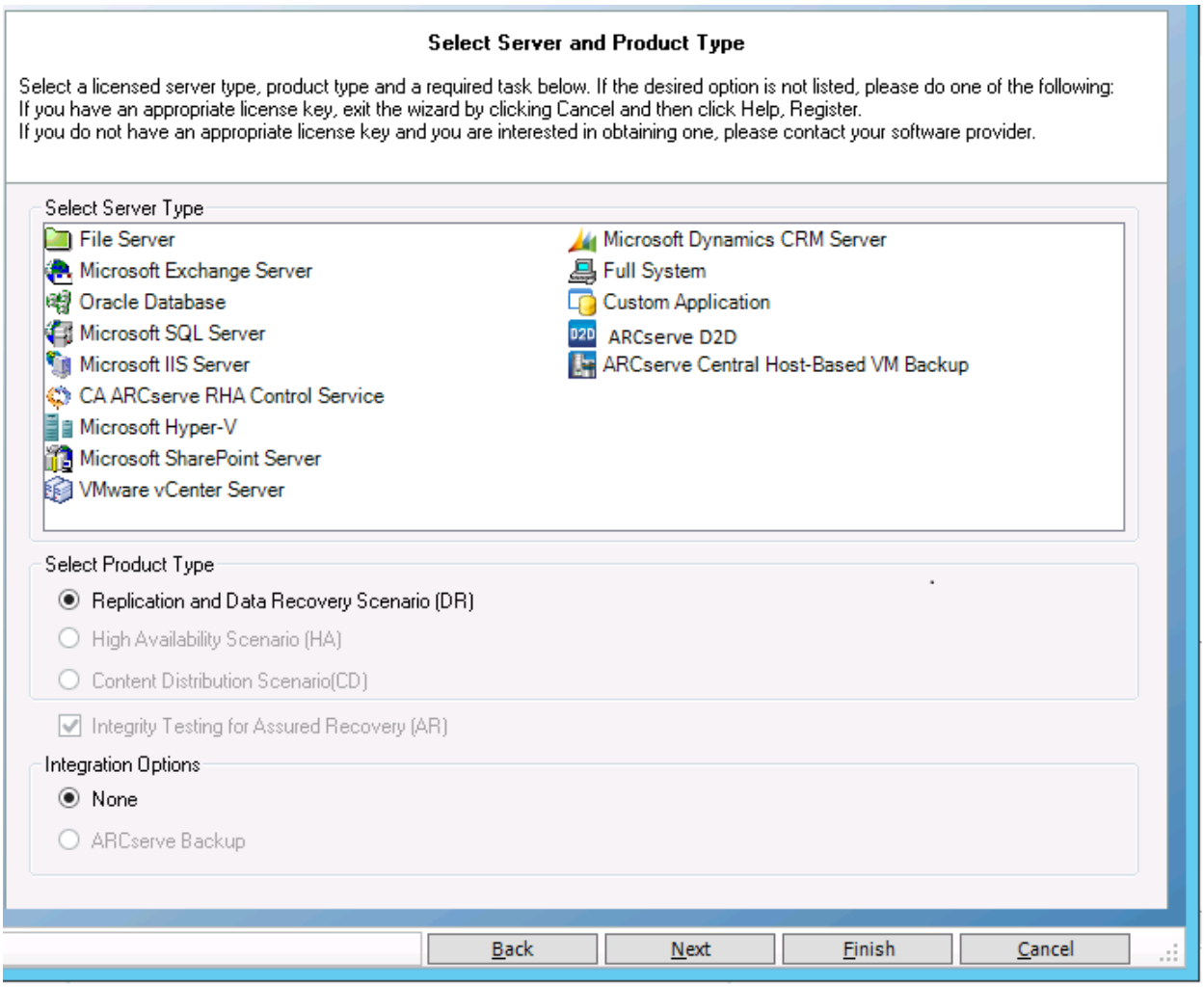
Per creare un nuovo scenario High Availability per sistemi completi EC2

1. Aprire la Gestione, selezionare Scenario, Nuovo oppure fare clic sul pulsante Nuovo scenario per avviare la creazione guidata.

   Viene visualizzata la schermata iniziale.

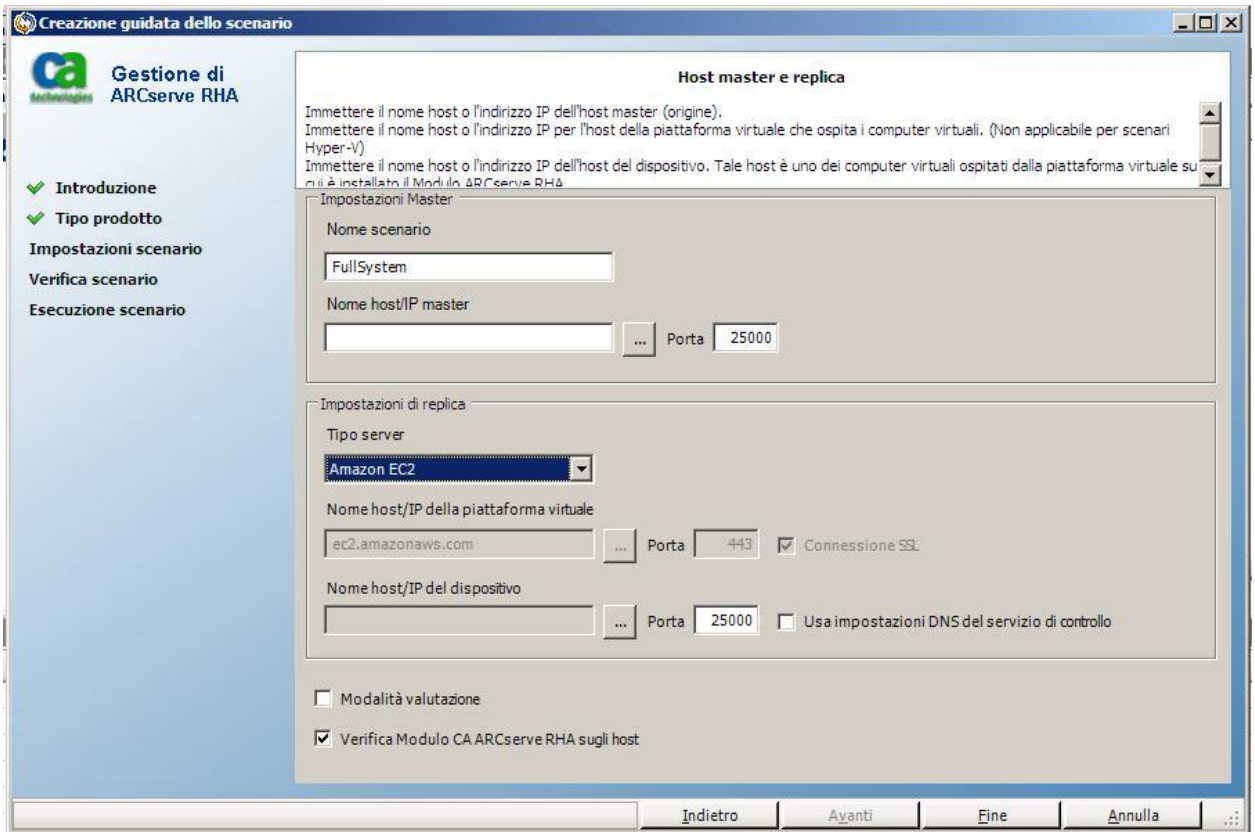
2. Scegliere Crea nuovo scenario, selezionare un gruppo dall'elenco e fare clic su Avanti.

Viene visualizzata la schermata Selezione del server e del tipo di prodotto.


Select Server and Product Type
Select a licensed server type, product type and a required task below. If the desired option is not listed, please do one of the following:
If you have an appropriate license key, exit the wizard by clicking Cancel and then click Help, Register.
If you do not have an appropriate license key and you are interested in obtaining one, please contact your software provider.
Select Server Type
File Server
Microsoft Exchange Server
Oracle Database
Microsoft SQL Server
Microsoft IIS Server
CA ARCserve RHA Control Service
Microsoft Hyper-V
Microsoft SharePoint Server
VMware vCenter Server
Microsoft Dynamics CRM Server
Full System
Custom Application
ARCserve D2D
ARCserve Central Host-Based VM Backup
Select Product Type
Replication and Data Recovery Scenario (DR)
High Availability Scenario (HA)
Content Distribution Scenario(CD)
Integrity Testing for Assured Recovery (AR)
Integration Options
None
ARCserve Backup
Back
Next
Finish
Cancel

3. Scegliere Sistema completo, Scenario High Availability (HA) e fare clic su Avanti.

Viene visualizzata la schermata Host master e replica.



4. Eseguire le seguenti operazioni nella schermata Host master e replica:

   a. Immettere un nome per lo scenario, il nome host o l'indirizzo IP e il numero di porta per il server master.

   b. Specificare Amazon EC2 come server di replica.

   c. Selezionare l'istanza di replica EC2 (dispositivo) Fare clic sul pulsante per individuare e selezionare l'account AWS e l'istanza di replica EC2 (dispositivo).

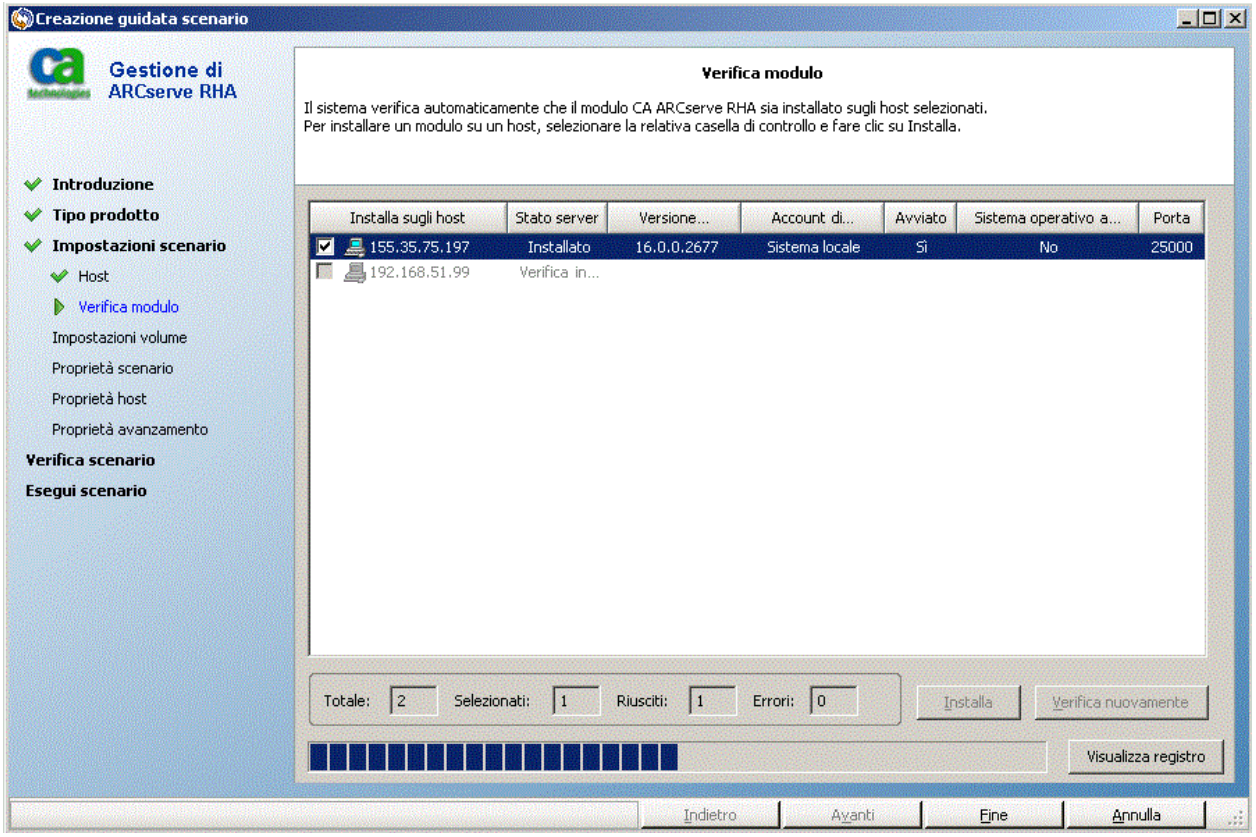
      Viene visualizzata la finestra di dialogo Selezione dell'istanza cloud.

   d. Selezionare l'account AWS, la replica cloud (dispositivo)e l'area, quindi fare clic su OK.

   e. Selezionare o deselezionare la casella di controllo Usa impostazioni DNS del servizio di controllo. Se si seleziona questa casella di controllo, le impostazioni DNS vengono applicate dal server del servizio di controllo all'host dell'istanza di replica EC2 (dispositivo).

   f. Assicurarsi che l'opzione Verifica Modulo Arcserve RHA sugli host sia abilitata (impostazione predefinita) e fare clic su Avanti.

Viene visualizzata la schermata Verifica modulo.



5. Attendere il completamento della verifica modulo e fare clic su Avanti. Se necessario, fare clic su Installa per aggiornare il modulo su uno o su entrambi i server, quindi fare clic su Verifica nuovamente.

   Viene visualizzata la schermata Impostazioni volume.

6. Selezionare uno o più volumi inclusi per il computer fisico che si desidera proteggere e fare clic su Avanti.

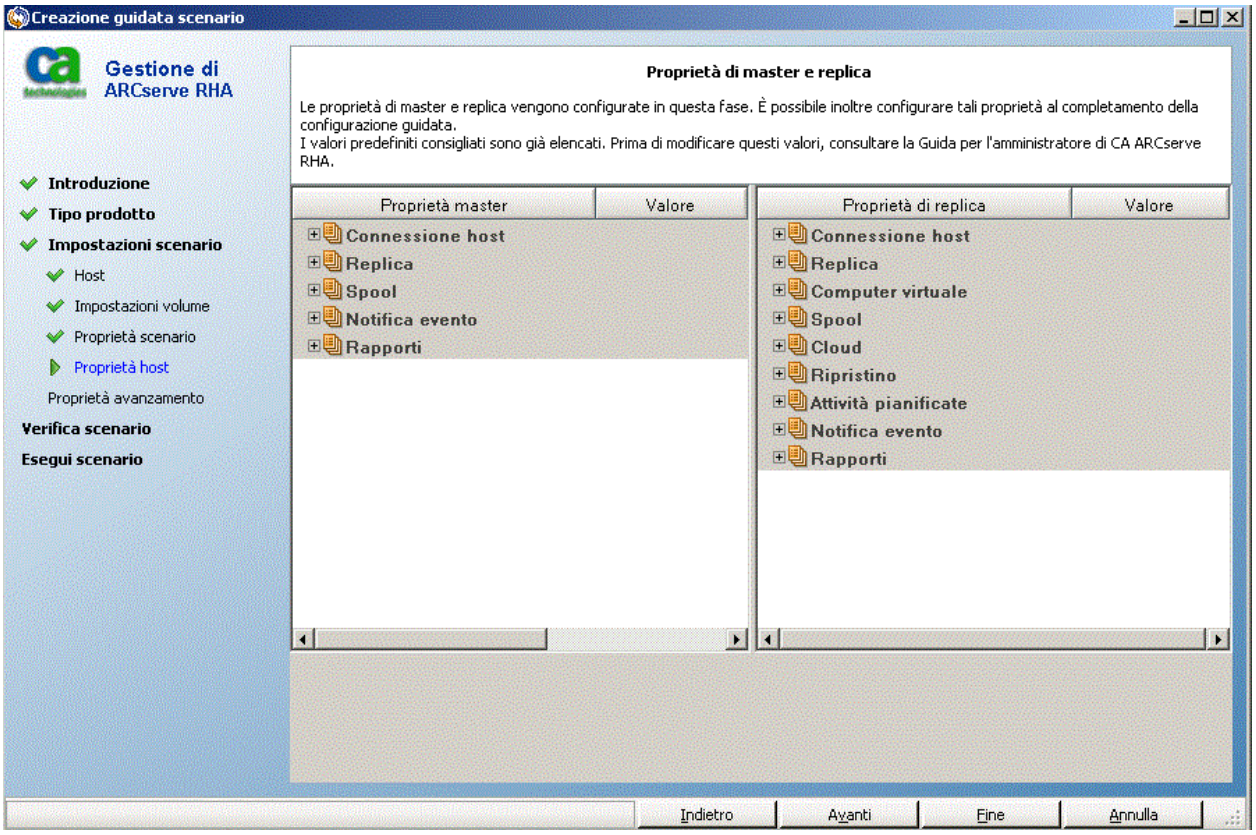
   Viene visualizzata la schermata Proprietà scenario.

7. Accettare i valori predefiniti oppure impostare nuovi valori e fare clic su Avanti.

   Nota: le proprietà dello scenario controllano l'intero scenario. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni, consultare la sezione Configurazione delle proprietà dello scenario (a pagina 201).

   Nota: la finestra di dialogo Mapping scheda di rete si apre se esiste più di una scheda di rete di replica.

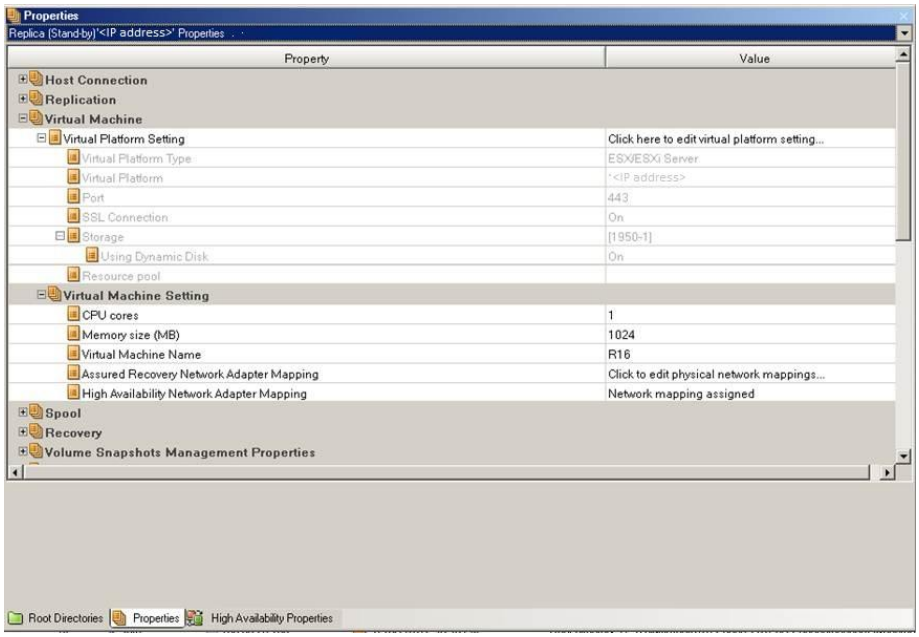
Viene visualizzata la schermata Proprietà di master e replica.



8. Le proprietà di master e replica sono applicabili solo ai server host. Accettare i valori predefiniti oppure modificare i valori in base alle proprie esigenze, e fare clic su Avanti.

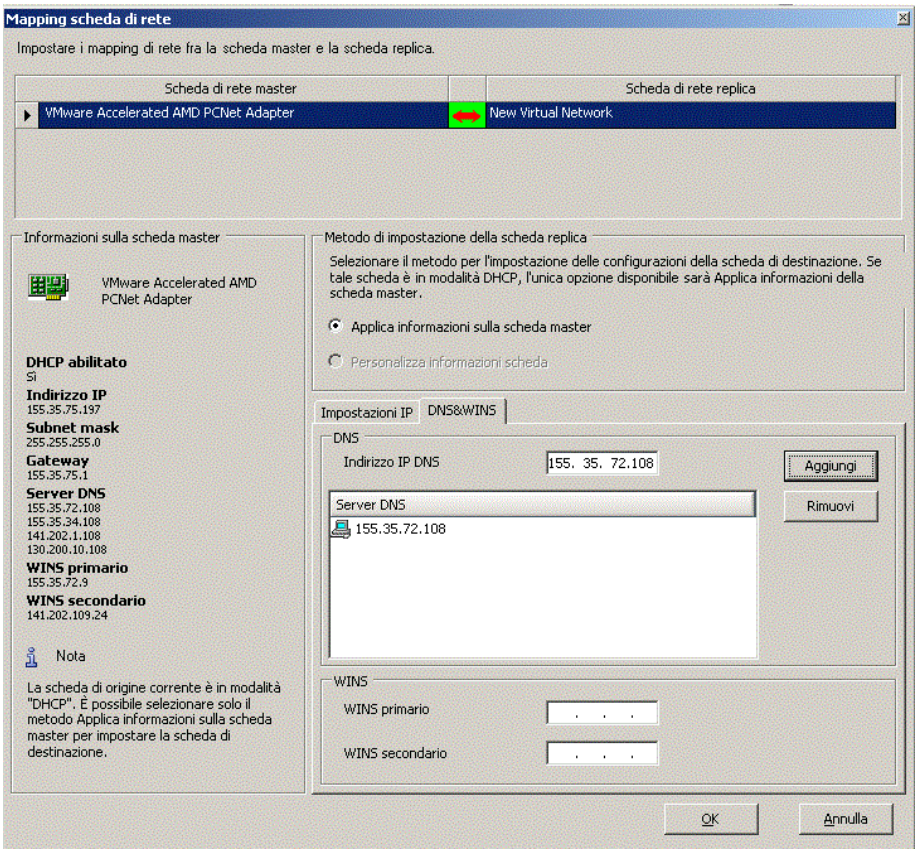
   Nota: tutte le proprietà di Replica cloud sono di sola lettura, fatta eccezione per la proprietà *Pulizia delle risorse cloud durante la rimozione dello scenario*, disattivata per impostazione predefinita.

   Per modificare il mapping di rete, espandere l'opzione Mapping di rete fisica da Computer virtuale.



Fare clic su Mapping scheda di rete Assured Recovery o Mapping scheda di rete High Availability.

Viene visualizzata la finestra di dialogo Mapping scheda di rete.



Impostare il mapping di rete tra la scheda master e la scheda di replica, quindi fare clic su OK.

Viene visualizzata la schermata Proprietà di master e replica.

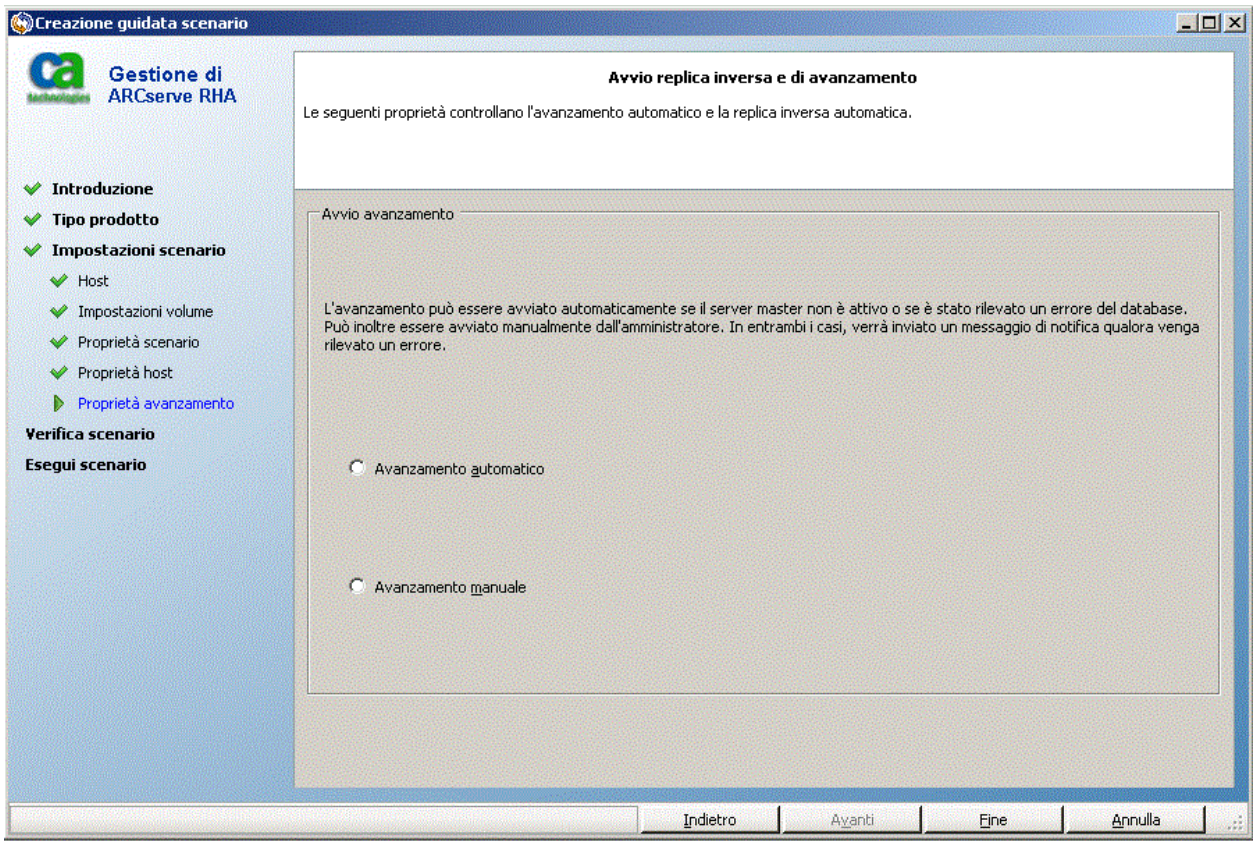
Fare clic su Avanti.

Viene visualizzata la schermata Proprietà avanzamento.

9. Espandere la proprietà*Avanzamento* e immettere il Nome host avanzamento.
10. Espandere la proprietà*Host* e immettere il Nome master completo e il Nome completo di replica.
11. Espandere la proprietà *Reindirizzamento traffico di rete* e specificare le opzioni di reindirizzamento, incluse Reindirizza DNS Indirizzi IP dei server DNS e Indirizzi IP di master in DNS.

    Nota: se l'opzione Reindirizza DNS viene impostata su *Non attivo* è possibile specificare un valore per l'opzione IP del computer virtuale sul server replica in DNS. Se il valore della proprietà Reindirizza DNS è impostato su *Attivo*, l'opzione IP del computer virtuale sul server replica in DNS non viene inclusa nell'elenco.

Viene visualizzata la schermata Avvio replica inversa e di avanzamento.


Creazione guidata scenario
Gestione di ARCserve RHA
Introduzione
Tipo prodotto
Impostazioni scenario
Host
Impostazioni volume
Proprietà scenario
Proprietà host
Proprietà avanzamento
Verifica scenario
Esegui scenario
Avvio replica inversa e di avanzamento
Le seguenti proprietà controllano l'avanzamento automatico e la replica inversa automatica.
Avvio avanzamento
L'avanzamento può essere avviato automaticamente se il server master non è attivo o se è stato rilevato un errore del database. Può inoltre essere avviato manualmente dall'amministratore. In entrambi i casi, verrà inviato un messaggio di notifica qualora venga rilevato un errore.
Avanzamento automatico
Avanzamento manuale
Indietro
Avanti
Fine
Annulla

12. Selezionare un'opzione di avanzamento. Non è consigliabile impostare l'avvio automatico. Per ulteriori informazioni, consultare la sezione Avanzamento (a pagina 274). Fare clic su Avanti.

    Attendere il completamento della verifica scenario.

13. Se vengono segnalati errori o avvisi, risolverli prima di continuare. Una volta completate le operazioni, fare clic su Avanti.

    Viene visualizzata la schermata Esecuzione scenario.

14. Fare clic su Esegui ora per avviare la sincronizzazione e attivare lo scenario oppure su Fine per eseguire lo scenario in un secondo momento.

Creazione di un nuovo scenario di replica dei dati su EC2

È possibile creare uno scenario di replica dei dati su EC2 per utilizzare le istanze EC2 specificate nella Creazione guidata dello scenario come server di replica. Tale procedura avvia la creazione guidata degli scenari di replica dei dati, che guida l'utente attraverso i vari passaggi necessari. È possibile configurare le proprietà senza utilizzare la procedura guidata.

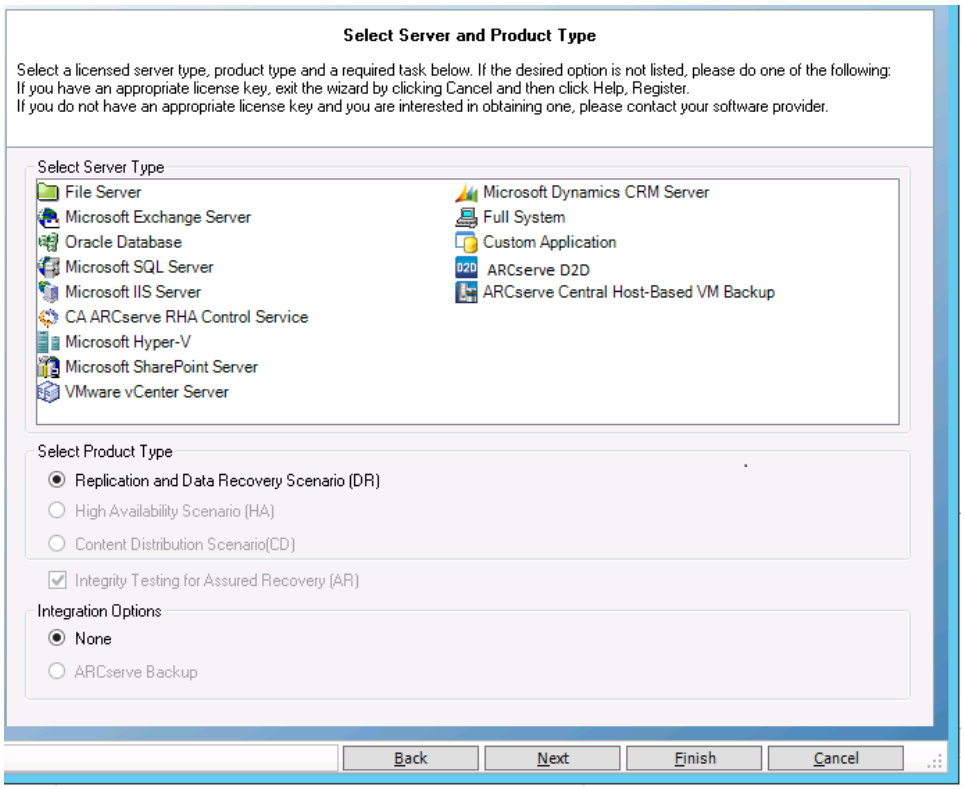
Per creare uno scenario di replica dei dati EC2

1. Aprire la Gestione, selezionare Scenario, Nuovo oppure fare clic sul pulsante Nuovo scenario per avviare la creazione guidata.

   Viene visualizzata la schermata iniziale.

2. Scegliere Crea nuovo scenario, selezionare un gruppo dall'elenco e fare clic su Avanti.

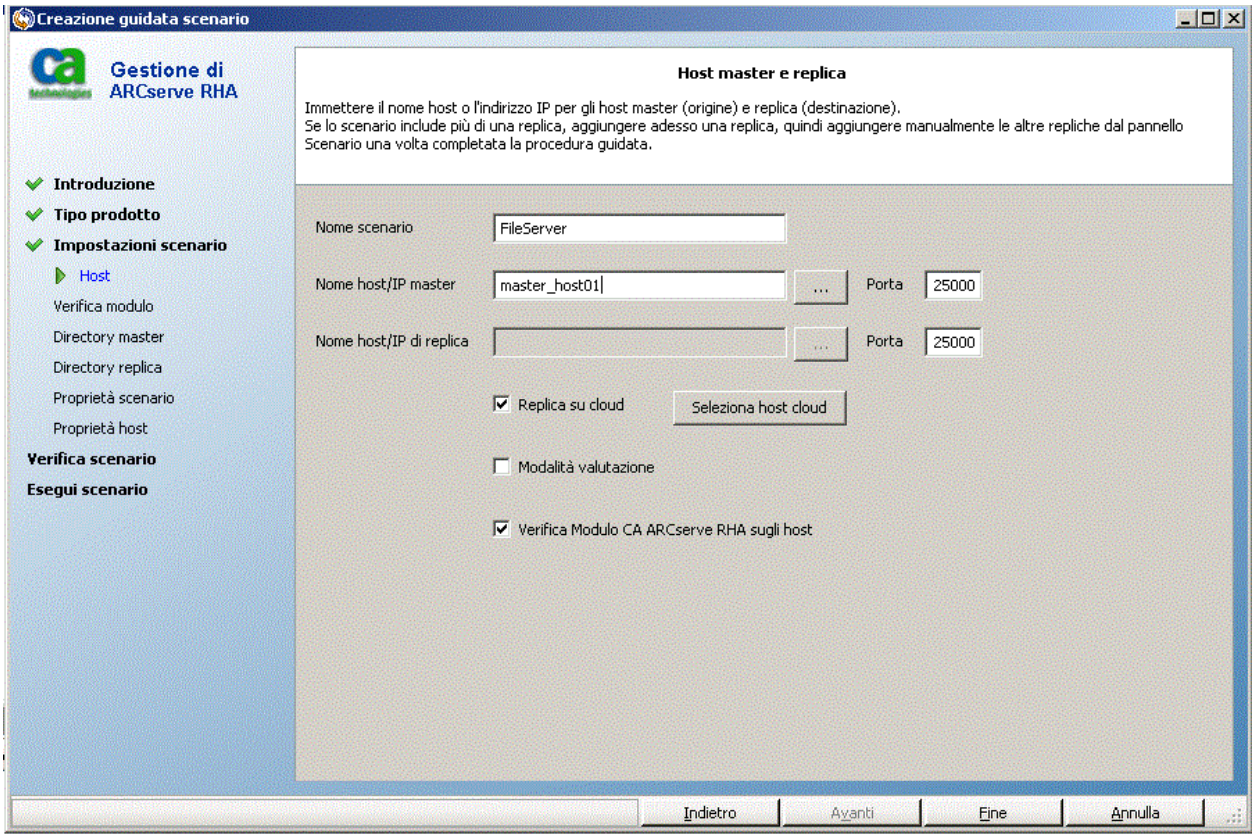
   Viene visualizzata la schermata Selezione del server e del tipo di prodotto.


Select Server and Product Type
Select a licensed server type, product type and a required task below. If the desired option is not listed, please do one of the following:
If you have an appropriate license key, exit the wizard by clicking Cancel and then click Help, Register.
If you do not have an appropriate license key and you are interested in obtaining one, please contact your software provider.
Select Server Type
File Server
Microsoft Exchange Server
Oracle Database
Microsoft SQL Server
Microsoft IIS Server
CA ARCserve RHA Control Service
Microsoft Hyper-V
Microsoft SharePoint Server
VMware vCenter Server
Microsoft Dynamics CRM Server
Full System
Custom Application
ARCserve D2D
ARCserve Central Host-Based VM Backup
Select Product Type
Replication and Data Recovery Scenario (DR)
High Availability Scenario (HA)
Content Distribution Scenario(CD)
Integrity Testing for Assured Recovery (AR)
Integration Options
None
ARCserve Backup
Back
Next
Finish
Cancel

1. Selezionare il tipo di server e lo Scenario di replica e ripristino dati (DR), quindi fare clic su Avanti.

   Nota: attualmente, Microsoft Hyper-V non è supportato negli scenari di replica basati su cloud.

Viene visualizzata la schermata Host master e replica.



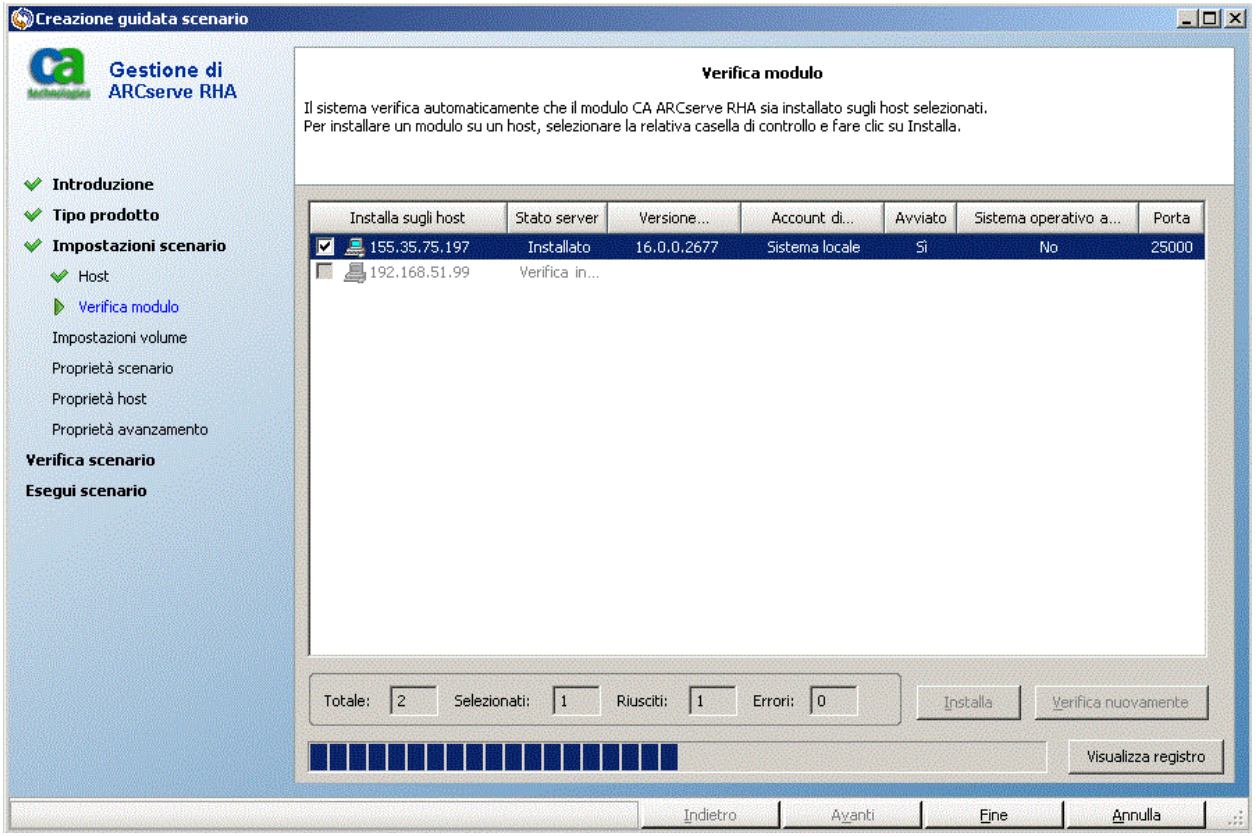
2. Immettere un nome per lo scenario, il nome host o l'indirizzo IP e il numero di porta per il server master. Specificare Amazon EC2 come server di replica. Selezionare la casella di controllo Replica su cloud e fare clic su Seleziona host cloud per specificare l'istanza di replica EC2 (dispositivo). Assicurarsi che l'opzione Verifica Modulo Arcserve RHA sugli host sia abilitata (impostazione predefinita), quindi fare clic su Avanti

   Viene visualizzata la finestra di dialogo Selezione dell'istanza cloud.

3. Immettere le informazioni relative al Fornitore cloud, all'Account cloud e all'Area, quindi fare clic su OK.

   Nota: fare clic sul pulsante Aggiorna per aggiornare l'elenco delle istanze.

Viene visualizzata la schermata Verifica modulo.



4. Attendere il completamento della verifica modulo e fare clic su Avanti. Se necessario, fare clic su Installa per aggiornare il modulo su uno o su entrambi i server, quindi fare clic su Verifica nuovamente.

   Viene visualizzata la schermata Impostazioni volume.

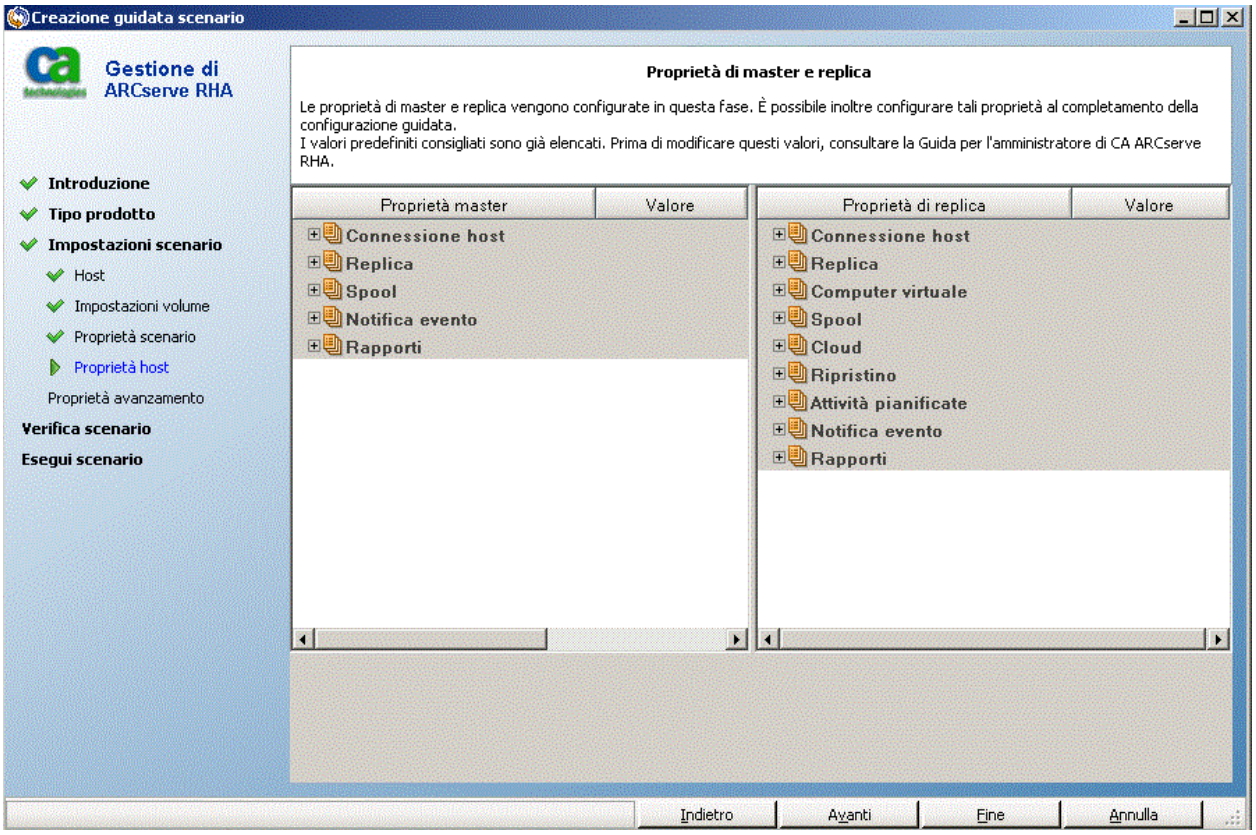
5. Immettere le informazioni e fare clic su Avanti.

   Viene visualizzata la schermata Proprietà scenario.

6. Accettare i valori predefiniti oppure impostare nuovi valori e fare clic su Avanti.

   Nota: le proprietà dello scenario controllano l'intero scenario. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni, consultare la sezione Configurazione delle proprietà dello scenario (a pagina 201).

Viene visualizzata la schermata Proprietà di master e replica.



7. Le proprietà del server master e di replica si applicano esclusivamente ai server host. Accettare i valori predefiniti oppure modificare i valori in base alle proprie esigenze, e fare clic su Avanti.

   Nota: tutte le proprietà della replica cloud sono disponibili in sola lettura, fatta eccezione per la proprietà *Arresta istanza quando lo scenario viene interrotto*, disattivata per impostazione predefinita. Per ulteriori informazioni, consultare la sezione Proprietà cloud (a pagina 231).

8. Fare clic su Avanti.

   Attendere il completamento della verifica scenario.

9. Se vengono segnalati errori o avvisi, risolverli prima di continuare. Una volta completate le operazioni, fare clic su Avanti.

   Viene visualizzata la schermata Esecuzione scenario.

10. Fare clic su Esegui ora per avviare la sincronizzazione e attivare lo scenario oppure su Fine per eseguire lo scenario in un secondo momento.

Esecuzione e sincronizzazione di uno scenario Replication o High Availability per i dati di sistemi completi EC2

Dopo aver creato uno scenario, è necessario eseguirlo per avviare il processo di replica. Gli scenari High Availability per sistemi completi EC2 e gli scenari di replica dei dati vengono eseguiti secondo le modalità degli scenari Arcserve RHA, con le seguenti eccezioni:

- Per ciascun volume master replicato, il dispositivo Arcserve RHA crea e connette un volume EBS della stessa dimensione.
- Per ciascun volume master replicato viene eseguita la sincronizzazione iniziale con il volume EBS corrispondente sul dispositivo Arcserve RHA, è possibile selezionare la sincronizzazione a livello di volume, blocco o file.
- il flusso di replica viene unificato per tutti gli scenari Sistema completo. La replica viene eseguita a livello del file, e le modifiche apportate ai file system vengono applicate ai volumi EBS montati.

Nota: per informazioni sul processo di replica, consultare la sezione Esecuzione del processo di replica (a pagina 127).

Esecuzione dell'avanzamento per uno scenario High Availability per sistemi completi EC2

In caso di mancata risposta del server master in uno scenario High Availability per sistemi completi EC2, utilizzare una delle seguenti modalità:

- Avanzamento manuale
- Failover automatico

In Arcserve RHA è possibile attivare automaticamente l'avanzamento quando il server master risulta non disponibile (failover). In alternativa, Arcserve RHA può semplicemente avvisare l'utente del problema, di modo che questi possa avviare manualmente l'avanzamento dalla Gestione. Una volta attivato, manualmente o automaticamente, il processo di avanzamento stesso è completamente automatizzato.

Se si seleziona l'avanzamento manuale, nel caso in cui l'opzione di failover automatico sia attivata e il server principale non risponda, viene eseguito il failover automatico. Il processo di avanzamento per uno scenario High Availability per sistemi completi EC2 è identico al processo utilizzato nel caso di scenari non cloud, con le seguenti eccezioni:

- Il dispositivo EC2 RHA esegue e definisce lo stato dell'istanza EC2 di failover come interrotto utilizzando le immagini AMI preparate previamente (< carha > fornisce quattro AMI pubblici). L'istanza EC2 di failover viene avviata dall'AMI con la stessa versione del sistema operativo principale e architettura del processore (W2K3 o W2K8 and x86 o X86_64).
- Il volume di avvio dell'istanza EC2 di failover viene disconnesso e collegato al dispositivo EC2 RHA.
- Il driver Xen viene aggiunto al volume replicato.
  - I driver Xen del volume di avvio originale della replica di failover vengono copiati.
  - Viene eseguita la routine di aggiunta driver, che esegue il montaggio la modifica del Registro di sistema sul volume master replicato.
- Il volume di avvio dell'istanza EC2 di failover originale viene disconnessa ed eliminata dal computer in cui è stata eseguita la copia dei driver Xen.
- I volumi di replica del master vengono disconnessi e collegati all'istanza EC2 di failover.
- L'istanza EC2 di failover viene avviata.

Nota: per ulteriori informazioni sull'avanzamento, consultare gli argomenti della sezione Avanzamento e regressione (a pagina 259).

Esecuzione del recupero mediante una replica EC2 di failover

Se si esegue la replica di un sistema locale su un'istanza EC2 di replica e viene effettuato l'avanzamento manuale o il failover automatico, è possibile eseguire il recupero dei dati tramite l'istanza EC2 di replica di failover:

- Eseguire la replica dell'istanza del sistema completo EC2 su un ambiente virtuale diverso (ad esempio Xen/Hyper-V/ESX locale o su un dispositivo EC2 RHA)
- Eseguire il ripristino dei singoli set di dati tramite lo scenario di replica di file system.

L'esecuzione del recupero mediante una replica EC2 di failover è identica al processo utilizzato per gli scenario non cloud, con alcune eccezioni. Quando si verifica l'avanzamento o il failover e viene avviata un'istanza EC2 di failover, viene creato uno scenario di replica precedente contenente il dispositivo EC2 come nuovo host master e l'host locale come nuova replica:

- Viene quindi eseguito uno scenario precedente automatico o manuale che consente la sincronizzazione solo a livello di file o di blocchi.
- I file di sistema di Windows vengono esclusi dalla sincronizzazione/replica.
- È possibile modificare le directory di replica /hive del Registro di sistema prima di eseguire lo scenario precedente.
- Viene eseguita la replica del Registro di sistema.

Nota: per informazioni sul processo di recupero, consultare la sezione Recupero dei dati persi da una replica (a pagina 252).

Capitolo 5: Esecuzione del processo di replica

Questa sezione contiene i seguenti argomenti:

Avvio della replica (a pagina 127)
Interruzione della replica (a pagina 131)
Sincronizzazione dei server master e replica (a pagina 131)
Autenticazione host (a pagina 141)
Chiusura e apertura della Gestione durante la replica (a pagina 147)
Sospendi replica (a pagina 148)
Esecuzione di uno scenario in modalità di valutazione (a pagina 153)

Avvio della replica

Dopo aver creato uno scenario, è necessario eseguirlo per avviare il processo di replica. Di norma, prima che le modifiche apportate ai dati sul server master possano essere replicate sul server di replica, é necessario sincronizzare i server master e di replica. Di conseguenza, il primo passaggio dell'avvio di una replica consiste nella sincronizzazione dei server master e di replica. Dopo aver sincronizzato i server, verrà avviata automaticamente una replica in linea, che aggiornerà continuamente il server di replica con tutte le modifiche apportate sul server master.

Arcserve RHA consente l'esecuzione simultanea della sincronizzazione e della replica. In questo caso, i server sono sincronizzati mentre i file sono in uso e in corso di aggiornamento. Tutte le modifiche che si verificano sul master vengono catturate e mantenute in uno spool. Una volta completata la sincronizzazione, la replica si avvia e viene aggiornata con tali modifiche.

Nota: per l'esecuzione corretta del processo di replica verificare che l'utente che esegue il modulo disponga delle autorizzazioni di lettura sul server master e delle autorizzazioni di lettura e scrittura su ciascuna directory principale di replica e sui file inclusi, nonché su tutti gli host di replica presenti..

Per avviare la replica, procedere come segue:

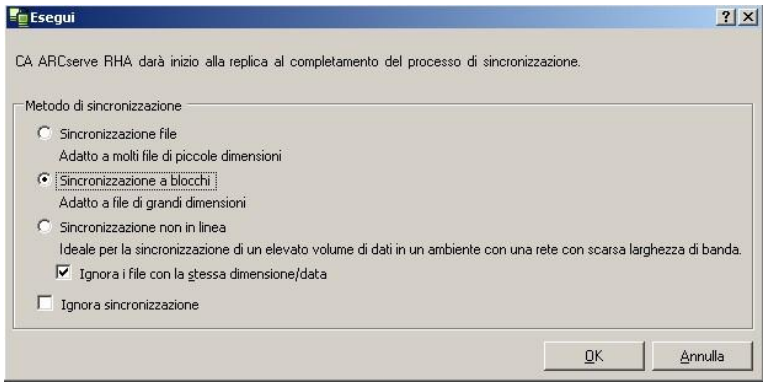
1. Dalla Gestione, selezionare lo scenario che si desidera eseguire.
2. Per eseguire lo scenario, fare clic su**Esegui** sulla barra degli strumenti standard. Arcserve RHA verifica lo scenario prima di procedere all'esecuzione.

3. Se lo scenario non è stato impostato correttamente oppure si sono verificati dei problemi negli host presenti, gli errori verranno segnalati nel riquadro Eventi.

   Prestare attenzione a quanto esposto di seguito:

   - Se vengono visualizzati errori, non è possibile eseguire lo scenario. È necessario correggere questi errori prima di poter avviare il processo di replica.
   - La replica dei punti di montaggio riuscirà solo se essi sono stati aggiunti al server master prima che il modulo venisse avviato. Se sono stati inclusi i punti di montaggio nelle directory principali master quando il modulo era già in esecuzione, non verrà segnalato alcun errore, ma la replica non sarà avviata. In questo caso, è necessario riavviare il modulo sul server master prima di iniziare la replica.
     Questa regola vale anche per la rimozione dei punti di montaggio durante la replica. Per rimuovere i punti di montaggio precedentemente definiti come parte della replica, procedere come segue: interrompere il modulo, rimuovere i punti di montaggio, e infine riavviare il modulo per procedere con il processo di replica.

4. Quando non viene restituito alcun errore, viene visualizzata la finestra di dialogo Esegui.


Esegui
CA ARCserve RHA darà inizio alla replica al completamento del processo di sincronizzazione.
Metodo di sincronizzazione
Sincronizzazione file
Adatto a molti file di piccole dimensioni
Sincronizzazione a blocchi
Adatto a file di grandi dimensioni
Sincronizzazione non in linea
Ideale per la sincronizzazione di un elevato volume di dati in un ambiente con una rete con scarsa larghezza di banda.
Ignora i file con la stessa dimensione/data
Ignora sincronizzazione
OK
Annulla

   Nella finestra di dialogo Esegui sono elencate le opzioni di sincronizzazione. È possibile scegliere tra: sincronizzazione file, sincronizzazione volume e sincronizzazione a blocchi. Per ulteriori informazioni, consultare la sezione Sincronizzazione (a pagina 131).

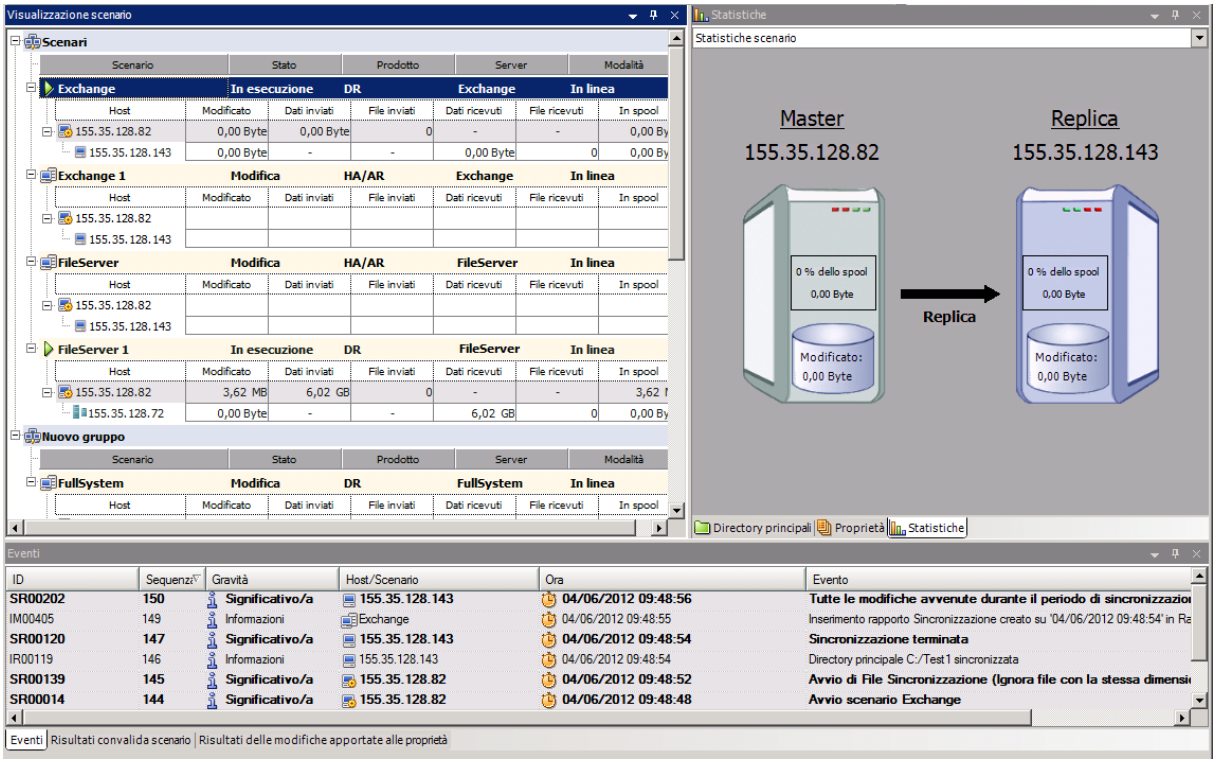
   Nota: in generale, i valori predefiniti sono la scelta più appropriata.

5. Per gli scenari file server, verificare che il metodo di sincronizzazione selezionato sia Sincronizzazione file e fare clic su OK.

   Importante: non saltare la sincronizzazione se non si ha la certezza assoluta che i dati nelle directory principali master e di replica sono identici.

   La Gestione ora indica che lo scenario è in esecuzione tramite il simbolo di riproduzione di colore verde posto a sinistra dello scenario e lo stato dello scenario, che diventa In esecuzione:

6. Dopo l'avvio dello scenario, alla base del riquadro Struttura viene visualizzata la scheda Statistiche, che contiene una rappresentazione grafica della replica.



7. Per impostazione predefinita, dopo l'avvio di una sincronizzazione, viene generato un Rapporto di sincronizzazione. Per visualizzare il rapporto, consultare la sezione Visualizzazione di un rapporto (a pagina 167).

   Nota: è anche possibile generare un Rapporto di replica (a pagina 169) periodicamente per monitorare il processo di replica su ciascun server presente.

Modalità di esecuzione

Quando la replica è in esecuzione e si seleziona lo scenario in esecuzione, la schermata della Gestione diventa di colore grigio. Le statistiche vengono visualizzate nel riquadro Struttura a destra. Gli eventi vengono registrati nel riquadro Eventi in basso. Se lo si desidera, è possibile modificare alcune proprietà durante l'esecuzione dello scenario. Consultare la sezione Modifica della configurazione di scenario (a pagina 240).

Nota: nelle procedure relative a cluster Arcserve RHA non supporta la ridenominazione di un gruppo di cluster durante l'esecuzione del modulo. Per assicurare il corretto funzionamento dei cluster con Arcserve RHA, arrestare il modulo prima di rinominare un gruppo di cluster.

Esecuzione di uno scenario mediante un server proxy

In casi in cui la configurazione di una rete privata virtuale non è possibile, Arcserve RHA consente la replica mediante server proxy. È possibile utilizzare un server proxy se l'host master risiede dietro un firewall che dispone soltanto dell'accesso proxy HTTP e l'host di replica risiede nell'Internet pubblico.

Importante. Un server di replica sull'Internet pubblico comporta dei rischi che dovranno essere valutati da ciascun utente prima di eseguire l'implementazione di uno scenario mediante un server proxy.

Per configurare uno scenario che utilizza un server proxy, immettere i dettagli del proxy nella proprietà Connessione host del server master.

Nota: dopo aver abilitato le impostazioni proxy sul server master, la replica verrà avviata automaticamente utilizzando il server proxy. Se non si desidera che la replica utilizzi il server proxy, disabilitare l'opzione Abilita server proxy HTTP.

Procedere come descritto di seguito:

1. Selezionare lo scenario in Gestione.
2. Selezionare l'host master e fare clic sulla proprietà Connessione host.
3. Attivare le informazioni proxy HTTP ed immettere i dettagli del server proxy, quale nome host, numero di porta e credenziali utente.
4. Eseguire lo scenario

Interruzione della replica

È necessario interrompere uno scenario in esecuzione per impostarne o modificarne le proprietà.

Per interrompere la replica, procedere come segue:

1. Dal riquadro Scenario, selezionare lo scenario che si desidera interrompere.
2. Per interrompere lo scenario, fare clic su Interrompi sulla barra degli strumenti standard.

   Viene visualizzato un messaggio di conferma in cui viene richiesto di confermare l'interruzione dello scenario.
3. Fare clic su Sì nel messaggio di conferma. Lo scenario viene interrotto.

   Dopo aver interrotto lo scenario, nella Gestione non verrà più visualizzato il simbolo di riproduzione di colore verde a sinistra dello scenario e lo stato dello scenario diventerà Interrotto dall'utente. Inoltre, la scheda Statistiche non sarà più disponibile nel riquadro Struttura.

Sincronizzazione dei server master e replica

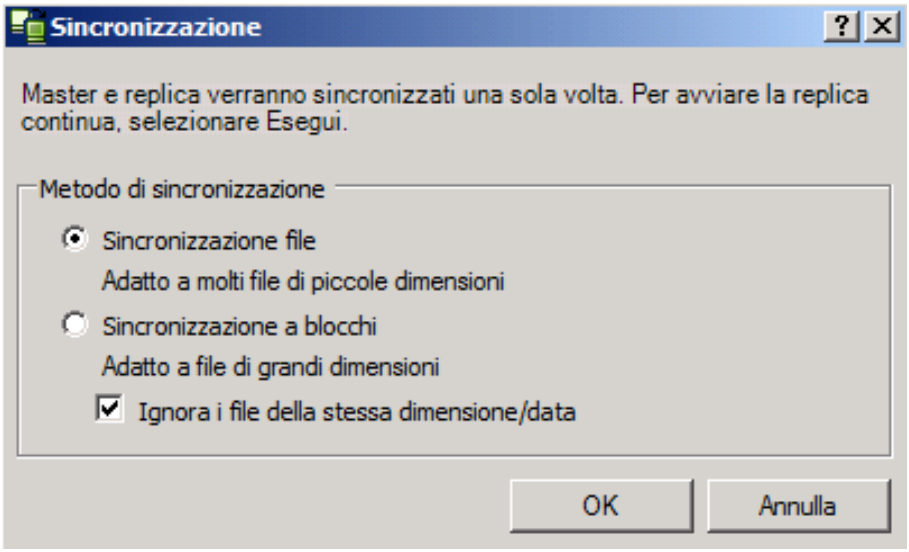
Il processo di sincronizzazione può essere attivato manualmente in qualsiasi momento, indipendentemente dall'esecuzione della replica. Si consiglia di eseguire la sincronizzazione manuale nelle seguenti situazioni:

- Prima di avviare la replica sui server con elevate quantità di dati e un rapporto di aggiornamento intensivo.
- Dopo un errore di rete che ha richiesto molto tempo, se la sincronizzazione automatica non è attivata.
- Dopo aver riavviato uno dei server facenti parte del processo, se la sincronizzazione automatica non è attivata.

Per sincronizzare i server master e di replica:

1. Dalla Gestione, selezionare lo scenario che si desidera sincronizzare.
2. Fare clic su Sincronizza sulla barra degli strumenti standard oppure selezionare l'opzione Sincronizza dal menu Strumenti.

   Viene visualizzata la finestra di dialogo Sincronizzazione contenente le opzioni di sincronizzazione.


Sincronizzazione
Master e replica verranno sincronizzati una sola volta. Per avviare la replica continua, selezionare Esegui.
Metodo di sincronizzazione
Sincronizzazione file
Adatto a molti file di piccole dimensioni
Sincronizzazione a blocchi
Adatto a file di grandi dimensioni
Ignora i file della stessa dimensione/data
OK
Annulla

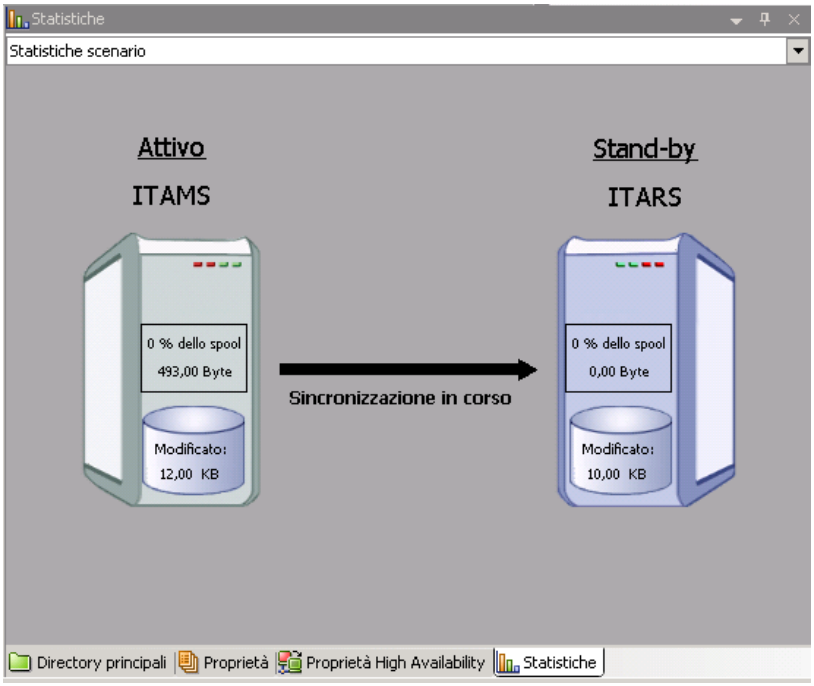
3. Scegliere le opzioni desiderate Per ulteriori informazioni sui metodi di sincronizzazione, consultare la sezione Metodi di sincronizzazione (a pagina 18).

   Nota: è inoltre possibile impostare l'esecuzione automatica della sincronizzazione a orari pianificati in giorni specifici ed escluderla in date specifiche. Per ulteriori informazioni, consultare la sezione Pianificazione della sincronizzazione (a pagina 211).

   Fare clic su OK per avviare la sincronizzazione in funzione del metodo selezionato.

Nota: è possibile eseguire un comando di sincronizzazione quando un server di replica è sospeso. Tuttavia, esso verrà eseguito solo dopo la ripresa della replica.

Dopo aver avviato il processo di sincronizzazione, viene visualizzata la scheda Statistiche, in cui si indica che la sincronizzazione è in corso.



Informazioni aggiuntive:

- Metodi di sincronizzazione (a pagina 18)
- Funzionamento della sincronizzazione non in linea (a pagina 133)
- Pianificazione della sincronizzazione (a pagina 211)

Funzionamento della sincronizzazione non in linea

La sincronizzazione non in linea consente di copiare i dati da replicare su una periferica esterna, quindi dalla periferica al server di replica. La sincronizzazione non in linea è un metodo efficace per trasferire grandi volumi di dati con una larghezza di banda di rete limitata.

Quando si utilizza la sincronizzazione non in linea, tenere presente quanto segue:

- Calcolare il tasso di modifica giornaliero dei dati protetti sul server master e moltiplicare tale valore per il numero di giorni necessari al server di replica per ricevere i dati. Ad esempio, se il tasso di modifica giornaliero è 2 GB e sono necessari 3 giorni per poter applicare i dati alla Replica, la dimensione di spool sulla Replica sarà circa 6 GB. È possibile eseguire scenari in modalità di valutazione per ricavare tali informazioni.

- Lo spool deve disporre di spazio a sufficienza per contenere il valore rilevato durante la valutazione. Se lo spool si riempie, sarà necessario riavviare gli scenari.
- Selezionare Continua sincronizzazione non in linea senza verificare i dati copiati sulla replica, a meno di essere sicuri che lo strumento di copia utilizzato per il trasferimento della snapshot alla replica mantenga tutti gli attributi di protezione. Le proprietà degli elenchi di controllo devono essere identiche dopo le operazioni di copia, in modo tale che la Sincronizzazione non in linea venga completata correttamente. Gli attributi di protezione potrebbero non corrispondere se l'opzione di verifica viene utilizzata con strumenti di copia normali. Si consiglia di non utilizzare Windows Explorer in quanto potrebbe modificare gli attributi di protezione.

  Nota: non è possibile utilizzare la sincronizzazione non in linea per scenari con repliche pianificate o per scenari in cui il Master corrisponde a un host UNIX/Linux.

Sarà, però, possibile procedere alla sincronizzazione non in linea per tutti gli altri tipi di scenari. Gli esempi riportati a continuazione mostrano il funzionamento della sincronizzazione non in linea per tali scenari.

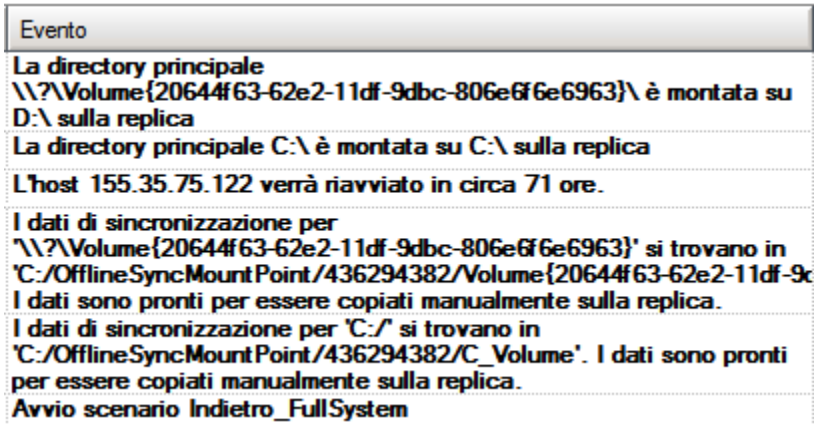
- High Availability per sistemi completi (a pagina 135)
- High Availability per sistemi non completi (a pagina 137)
- Scenario di sistema completo precedente o di ripristino bare metal (a pagina 138)

Esecuzione di scenari High Availability per sistemi completi

Utilizzare questo metodo di sincronizzazione non in linea in caso di set di dati di produzione di grandi dimensioni e se la velocità effettiva del collegamento WAN non è sufficiente per eseguire la sincronizzazione dell'intero set di dati in un periodo di tempo ragionevole.

Il processo di sincronizzazione non in linea crea snapshot VSS del volume che risiede nella directory principale del server master. Per impostazione predefinita, Arcserve RHA monta la directory principale nella posizione di installazione del modulo RHA, ad esempio l'unità C:\. L'esempio seguente mostra la posizione dei file snapshot VSS durante l'esecuzione del processo di sincronizzazione non in linea:

```
C:\OfflineSyncMountPoint\<scenarioID>\E_volume
```


Evento
La directory principale \\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}\ è montata su D:\ sulla replica
La directory principale C:\ è montata su C:\ sulla replica
L'host 155.35.75.122 verrà riavviato in circa 71 ore.
I dati di sincronizzazione per '\\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}' si trovano in 'C:/OfflineSyncMountPoint/436294382/Volume{20644f63-62e2-11df-9c
I dati sono pronti per essere copiati manualmente sulla replica.
I dati di sincronizzazione per 'C:/' si trovano in 'C:/OfflineSyncMountPoint/436294382/C_Volume'. I dati sono pronti per essere copiati manualmente sulla replica.
Avvio scenario Indietro_FullSystem

Per il server di replica, creare un altro scenario di disaster recovery di file server da replicare dalla periferica esterna nella directory principale di destinazione. Ad esempio, E:\Data sul server di replica. Se lo si desidera, è possibile eseguire una Robocopy, (copia di file efficace), una copia di file o qualsiasi altro tipo di copia dal volume di snapshot montato sul server master e copiare manualmente i dati dall'unità esterna alla cartella di destinazione sul server di replica, dopo aver trasferito l'unità.

Procedere come descritto di seguito:

1. Configurare uno scenario secondo la procedura abituale.
2. Quando si raggiunge l'ultimo passaggio della Procedura guidata di creazione scenario, non faccia fare clic su Esegui ora. Fare clic su Fine.
3. Dalla Gestione, fare clic su Esegui. Viene visualizzata la finestra di dialogo Esegui.

4. Selezionare Sincronizzazione non in linea, quindi fare clic su OK.

   Dopo l'avvio dello scenario, la console eventi visualizza il percorso ai dati per l'esecuzione della copia manuale. Arcserve RHA acquisisce una snapshot VSS, consentendo di eseguire la copia senza ripercussioni sul set di dati di produzione.

   a. Il volume master genera un servizio Copia Shadow del volume. Tali dati si trovano in C:\OfflineSyncMountPoint\<ID scenario>\.

      Nota: è possibile personalizzare il volume principale mediante la configurazione del valore SnapshotStorageVolume in ws_rep.cfg.

   b. Il volume del disco viene generato e montato sulla replica come <percorso di installazione>\Modulo\computer virtuale\<ID volume>\.

   c. Copiare tutti i dati del master sul punto di montaggio di replica. Copiare manualmente i dati dal percorso VSS creato sul master su una periferica esterna o un supporto ottico (DVD-R, CD-R). Trasportare fisicamente il supporto esterno sul server di replica.

   Durante il trasporto, il set di dati di produzione memorizza qualsiasi modifica apportata ai dati di origine nello spool della replica.

5. Copiare i dati archiviati sul supporto esterno nella directory principale corrispondente sul server di replica.

   Utilizzare un'utilità di copia, quale xcopy o fastcopy, per copiare tutti i file e le cartelle del server master dalla cartella OfflineSyncMountPoint alla cartella di replica <percorso di installazione>\Modulo\computer virtuale\<ID scenario>\<Volume>.

   ```
   xcopy [Source] [Destination] /E /C /H /R
   ```

6. Una volta copiati i file, fare clic su Strumenti, Gestione sincronizzazione non in linea per aprire la finestra di dialogo corrispondente.

7. Selezionare o deselezionare la casella di controllo Ignora file della stessa dimensione/ora e fare clic su OK.

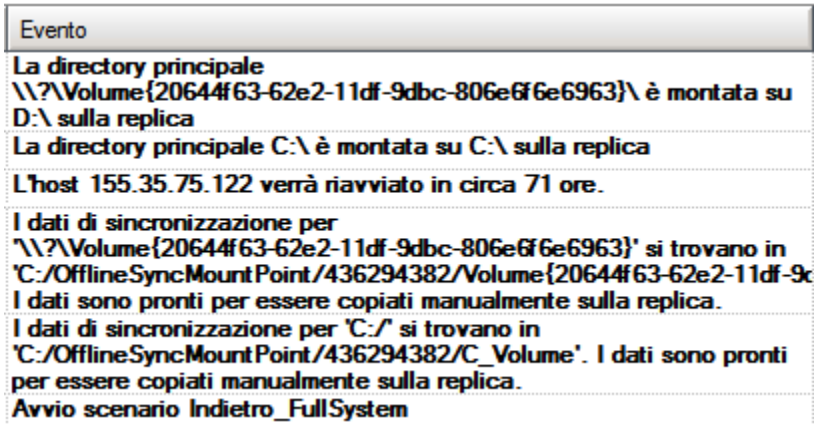
8. Quando il processo di sincronizzazione a blocchi viene avviato, gli eventi vengono visualizzati nella console eventi, mentre quando il processo viene completato, lo stato della sincronizzazione passa a Replica. Qualunque modifica memorizzata nello spool della replica durante la sincronizzazione non in linea passa, quindi, alla replica e viene cancellata dallo spool.

Esecuzione di scenari High Availability per sistemi non completi

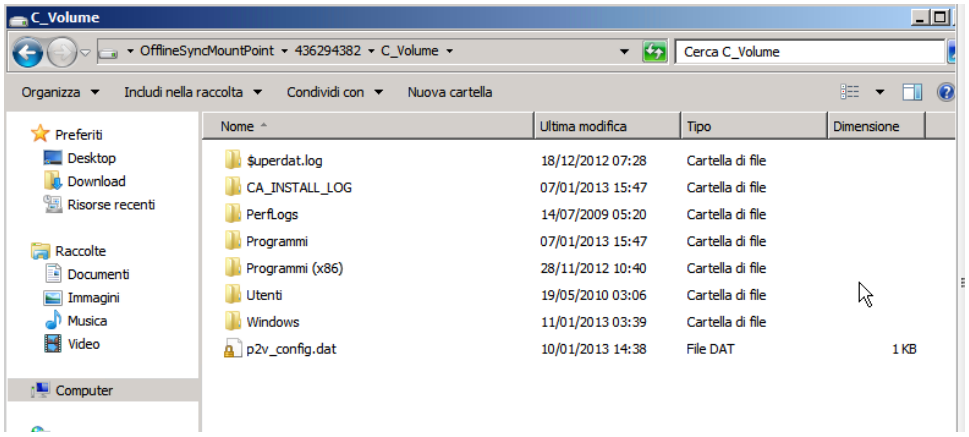
Utilizzare questo metodo di sincronizzazione non in linea in caso di set di dati di produzione di grandi dimensioni e se la velocità effettiva del collegamento WAN non è sufficiente per eseguire la sincronizzazione dell'intero set di dati in un periodo di tempo ragionevole.

Il processo di sincronizzazione non in linea crea snapshot VSS del volume che risiede nella directory principale del server master. Per impostazione predefinita, Arcserve RHA monta la directory principale nella posizione di installazione del modulo RHA, ad esempio l'unità C:\. L'esempio seguente mostra la posizione dei file snapshot VSS durante l'esecuzione del processo di sincronizzazione non in linea:

```
C:\OfflineSyncMountPoint\<scenarioID>\E_volume
```


Evento
La directory principale \\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}\ è montata su D:\ sulla replica
La directory principale C:\ è montata su C:\ sulla replica
L'host 155.35.75.122 verrà riavviato in circa 71 ore.
I dati di sincronizzazione per '\\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}' si trovano in 'C:/OfflineSyncMountPoint/436294382/Volume{20644f63-62e2-11df-9c
I dati sono pronti per essere copiati manualmente sulla replica.
I dati di sincronizzazione per 'C:/' si trovano in 'C:/OfflineSyncMountPoint/436294382/C_Volume'. I dati sono pronti per essere copiati manualmente sulla replica.
Avvio scenario Indietro_FullSystem

Nota: nella finestra riportata di seguito, C_Volume rappresenta un volume VSS montato su questo punto. Ad esempio, quando si desidera memorizzare gli attributi di file sparse, è possibile creare un nuovo scenario disaster recovery di file server per replicare i dati dalla snapshot montata a una periferica esterna.



Per il server di replica, creare un altro scenario di disaster recovery di file server da replicare dalla periferica esterna nella directory principale di destinazione. Ad esempio, E:\Data sul server di replica. Se lo si desidera, è possibile eseguire una Robocopy, (copia di file efficace), una copia di file o qualsiasi altro tipo di copia dal volume di snapshot montato sul server master e copiare manualmente i dati dall'unità esterna alla cartella di destinazione sul server di replica, dopo aver trasferito l'unità.

Procedere come descritto di seguito:

1. Configurare lo scenario utilizzando la procedura abituale.
2. Da Gestione, fare clic su Gestione sincronizzazione non in linea.
3. Copiare i dati dalla snapshot VSS montata alla periferica esterna.
4. Trasferire la periferica sul server di replica e copiare i dati nella cartella di destinazione.
5. Dal menu Gestione, fare clic su Strumenti e Gestione sincronizzazione non in linea.
6. Selezionare l'opzione di sincronizzazione non in linea che si desidera utilizzare.

   Nota: l'opzione Verifica confronta i file della snapshot VSS montata disponibili sul server master con i dati della directory principale del server di replica e riporta eventuali differenze.
7. Continuare l'esecuzione dello scenario.

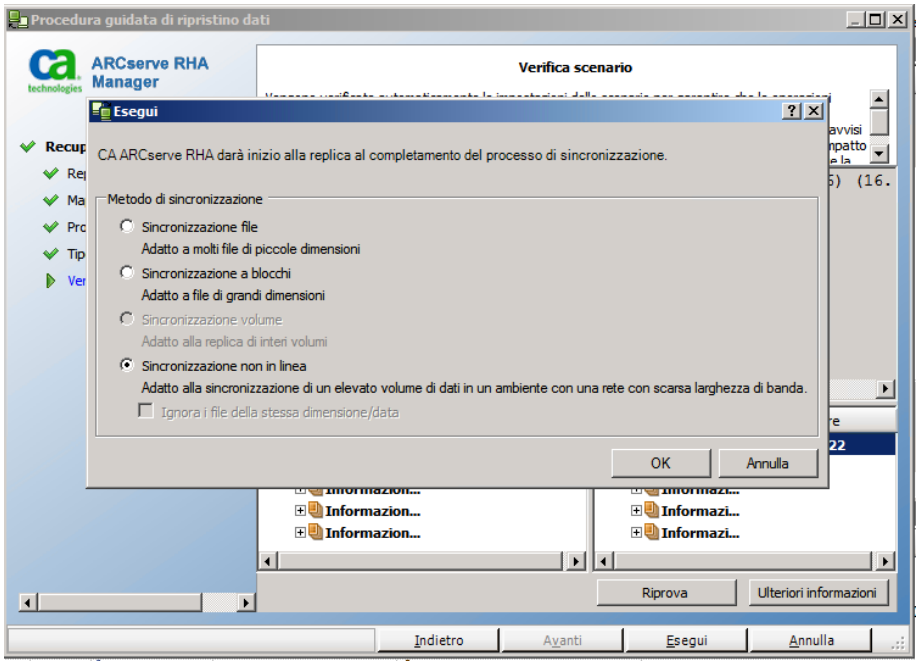
Esecuzione di scenari di sistema completo precedente e i ripristino bare metal

Utilizzare questo metodo di sincronizzazione per sincronizzare i dati di ripristino bare metal a livello di volume o di blocco.

Procedere come descritto di seguito:

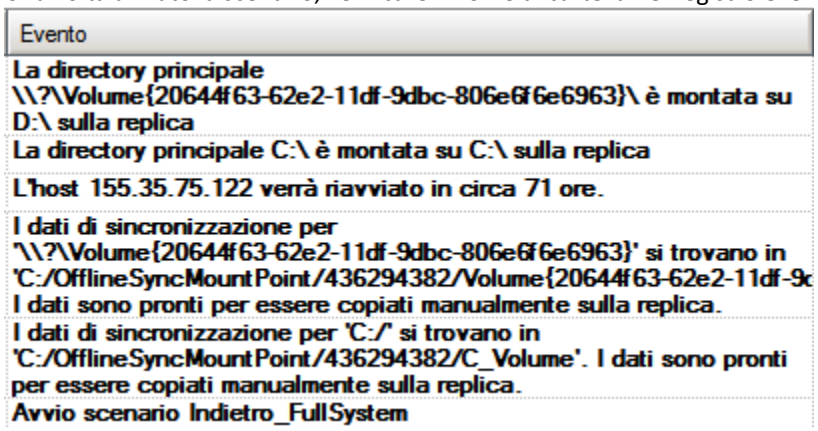
1. Eseguire lo scenario precedente o lo scenario di ripristino bare metal e immettere l'indirizzo IP di origine e di destinazione.

2. Quando viene raggiunta la fase finale della creazione guidata dello scenario, selezionare Sincronizzazione non in linea.


Procedura guidata di ripristino dati
ARCserve RHA Manager
Verifica scenario
Esegui
CA ARCserve RHA darà inizio alla replica al completamento del processo di sincronizzazione.
Metodo di sincronizzazione
Sincronizzazione file
Adatto a molti file di piccole dimensioni
Sincronizzazione a blocchi
Adatto a file di grandi dimensioni
Sincronizzazione volume
Adatto alla replica di interi volumi
Sincronizzazione non in linea
Adatto alla sincronizzazione di un elevato volume di dati in un ambiente con una rete con scarsa larghezza di banda.
Ignora i file della stessa dimensione/data
OK
Annulla
Riprova
Ulteriori informazioni
Indietro
Avanti
Esegui
Annulla

.

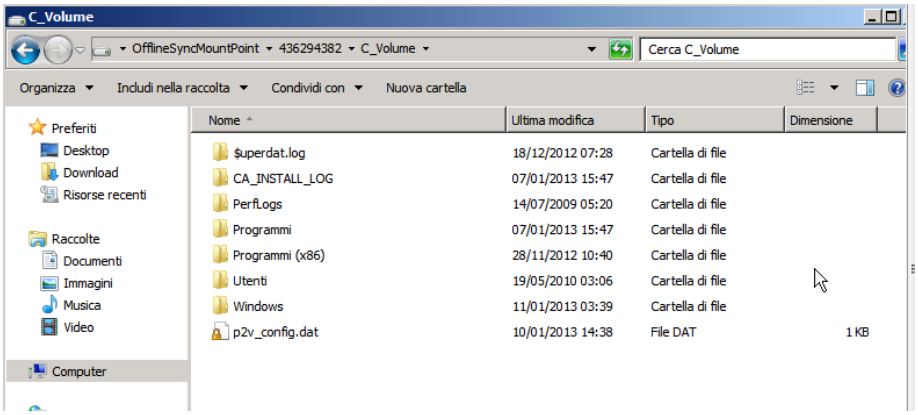
3. Una volta avviato la scenario, verificare il nome di cartella nel registro eventi.


Evento
La directory principale \\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}\ è montata su D:\ sulla replica
La directory principale C:\ è montata su C:\ sulla replica
L'host 155.35.75.122 verrà riavviato in circa 71 ore.
I dati di sincronizzazione per '\\?\Volume{20644f63-62e2-11df-9dbc-806e6f6e6963}' si trovano in 'C:/OfflineSyncMountPoint/436294382/Volume{20644f63-62e2-11df-9c
I dati sono pronti per essere copiati manualmente sulla replica.
I dati di sincronizzazione per 'C:/' si trovano in 'C:/OfflineSyncMountPoint/436294382/C_Volume'. I dati sono pronti per essere copiati manualmente sulla replica.
Avvio scenario Indietro_FullSystem

4. Accedere al server del dispositivo e individuare la cartella del punto di montaggio VSS.

   Per lo scenario di ripristino bare metal, accedere al server del dispositivo e individuare la cartella del punto di montaggio VSS.

   Per lo scenario precedente, eseguire l'accesso al computer virtuale generato mediante l'avanzamento e individuare la cartella del punto di montaggio VSS.



5. Copiare manualmente i dati dal percorso VSS creato sul server del dispositivo o sul computer virtuale generato mediante l'avanzamento su una periferica esterna o un supporto ottico (DVD-R, CD-R). Trasportare fisicamente il supporto esterno sul server di ripristino bare metal.

   Durante il trasporto, il set di dati di produzione memorizza qualsiasi modifica apportata ai dati di origine nello spool della replica.

6. Copiare i dati archiviati sul supporto esterno nella directory principale corrispondente sui volumi mappati sul server bare metal.

7. Utilizzare un'utilità di copia, ad esempio xcopy o fastcopy, per copiare tutti i file e le cartelle dal server del dispositivo al server ripristino bare metal.

   ```
   xcopy [Source] [Destination] /E /C /H /R
   ```

   Attendere il completamento del processo di copia.

8. Accedere alla Gestione di RHA e fare clic sul pulsante Gestione sincronizzazione non in linea.

   Viene avviato il processo di sincronizzazione a blocchi.

9. Una volta completata la sincronizzazione a blocchi, eseguire il processo di avanzamento.

Autenticazione host

Quando lo scenario viene creato ed eseguito, Arcserve RHA verifica le credenziali utente di tutti gli host. Arcserve RHA garantisce la creazione dei file di replica nella cartella corretta nel caso in cui più utenti eseguano la replica su un singolo server di replica. Il processo di autenticazione verifica che l'utente disponga delle autorizzazioni corrette per l'accesso alla propria cartella sul server di replica. In caso di errore della verifica della cartella o delle credenziali host, lo scenario viene interrotto immediatamente.

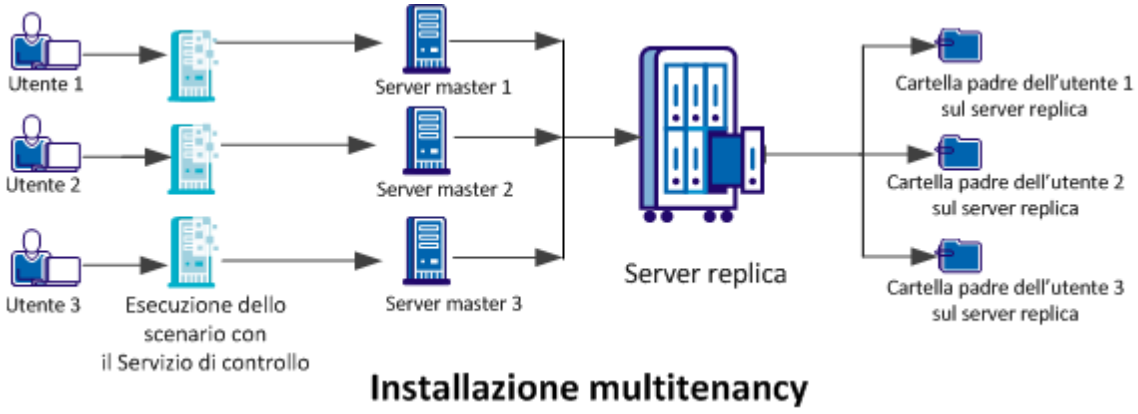
Abilitazione della replica multitenancy

In una installazione di replica multitenancy, viene eseguita la replica di più master appartenenti a clienti diversi su un singolo server di replica. Il server di replica appartiene a un service provider MSP e viene gestito da un amministratore MSP. L'utente finale possiede un Servizio di controllo Arcserve remoto (CS). Gli utenti creano scenari e dati di replica sul server di replica.

Sul server di replica, l'amministratore crea gli utenti, assegna la cartella padre della directory principale e concede le autorizzazioni di controllo completo per la cartella padre. Il nome utente, la password e i dettagli della cartella padre vengono condivisi con gli utenti. Gli utenti specificano questi dettagli durante la creazione dello scenario.

Gli utenti dispongono di un accesso limitato al computer di replica e dispongono delle autorizzazioni di controllo completo solamente per la propria cartella. Inoltre, gli utenti possono creare directory principali unicamente nella propria cartella.

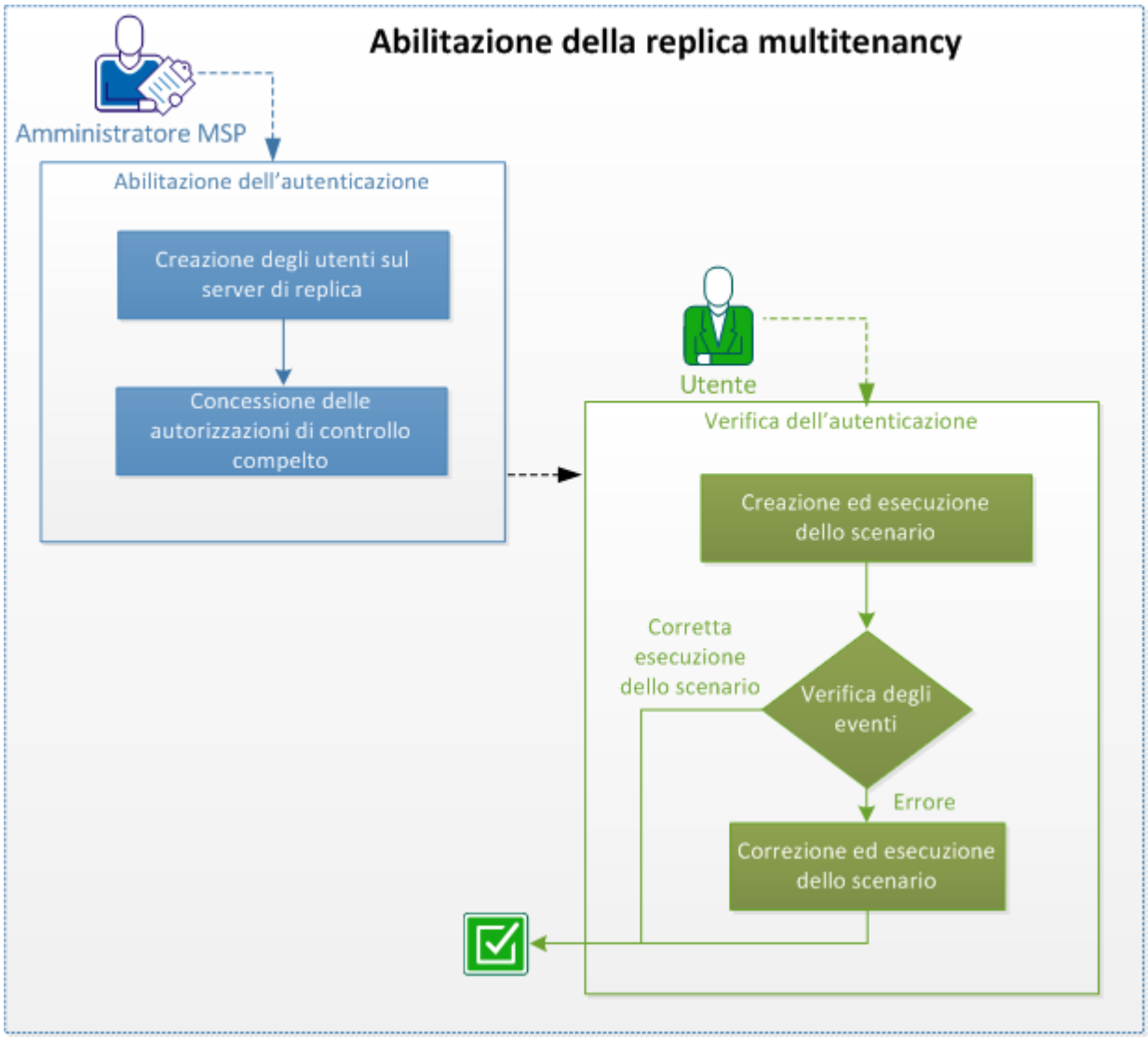
Il seguente diagramma mostra un'impostazione multitenancy:


Utente 1
Utente 2
Utente 3
Esecuzione dello scenario con il Servizio di controllo
Server master 1
Server master 2
Server master 3
Server replica
Cartella padre dell'utente 1 sul server replica
Cartella padre dell'utente 2 sul server replica
Cartella padre dell'utente 3 sul server replica
Installazione multitenancy

Procedura di abilitazione della replica multitenancy

Per abilitare la replica multitenancy, l'amministratore deve innanzitutto creare gli utenti nel server di replica e concedere le autorizzazioni di controllo completo per la cartella padre della directory principale. Quando un utente esegue lo scenario, Arcserve RHA verifica se l'utente dispone delle credenziali host corrette e delle autorizzazioni di controllo completo per la cartella padre. Lo scenario viene eseguito correttamente se entrambi questi criteri vengono soddisfatti. In caso contrario si verifica un errore e lo scenario viene interrotto.

Il diagramma seguente mostra la procedura per abilitare la replica multitenancy in un'installazione MSP.



Per abilitare la replica multitenancy, eseguire le attività seguenti:

Ruolo amministratore MSP

1. Creazione degli utenti sul server di replica (a pagina 143)
2. Concessione delle autorizzazioni di controllo completo (a pagina 144)

Ruolo utente

1. Creazione ed esecuzione dello scenario (a pagina 145)
2. Verifica degli eventi (a pagina 146)
3. Correzione ed esecuzione dello scenario (a pagina 146)

Creazione di utenti sul server di replica (Amministratore MSP)

L'amministratore crea gli utenti sul server di replica per ciascun utente. Inoltre, per ciascun utente, definisce la cartella padre che verrà utilizzata dall'utente per salvare le directory principali di replica contenenti i file replicati. L'amministratore può creare le cartelle in qualsiasi posizione. Ad esempio, è possibile creare le cartelle seguenti come cartelle padre.

C:\Uploads\User 1

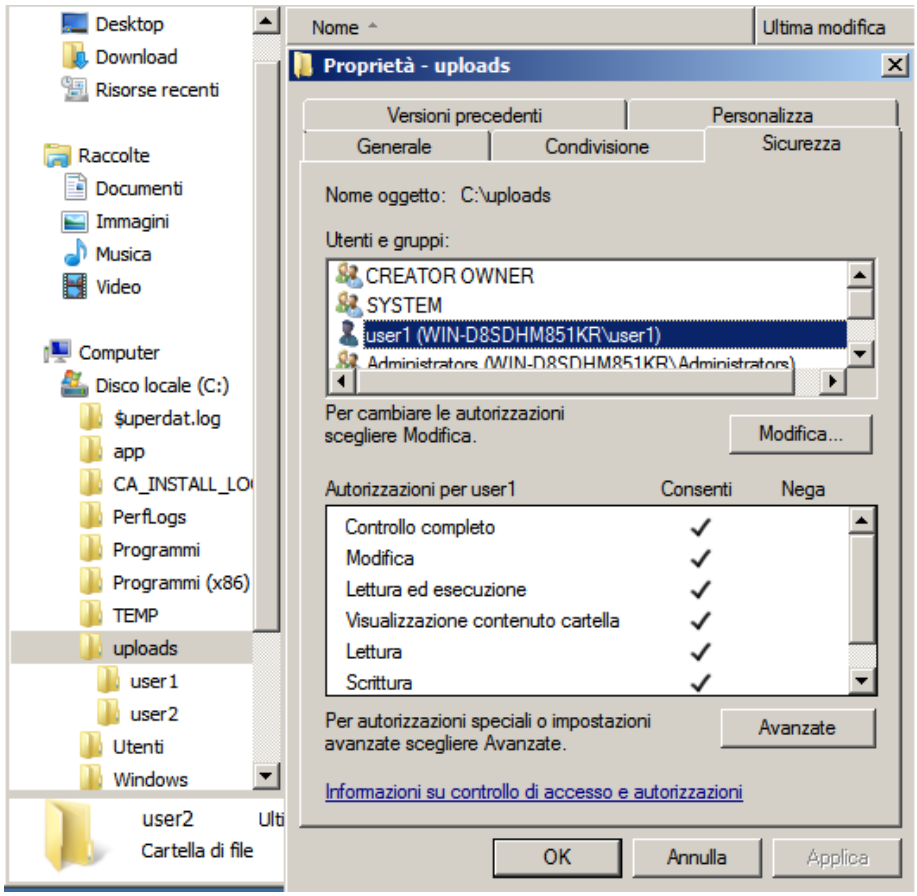
C:\Uploads\User 2

Concessione delle autorizzazioni di controllo completo (Amministratori MSP)

Dopo avere creato la cartella, verificare che ciascun utente esegua l'archiviazione dei file di replica nella cartella corrispondente. Concedere l'autorizzazione di controllo completo a ciascun utente per la cartella padre della directory principale corrispondente.

Procedere come descritto di seguito:

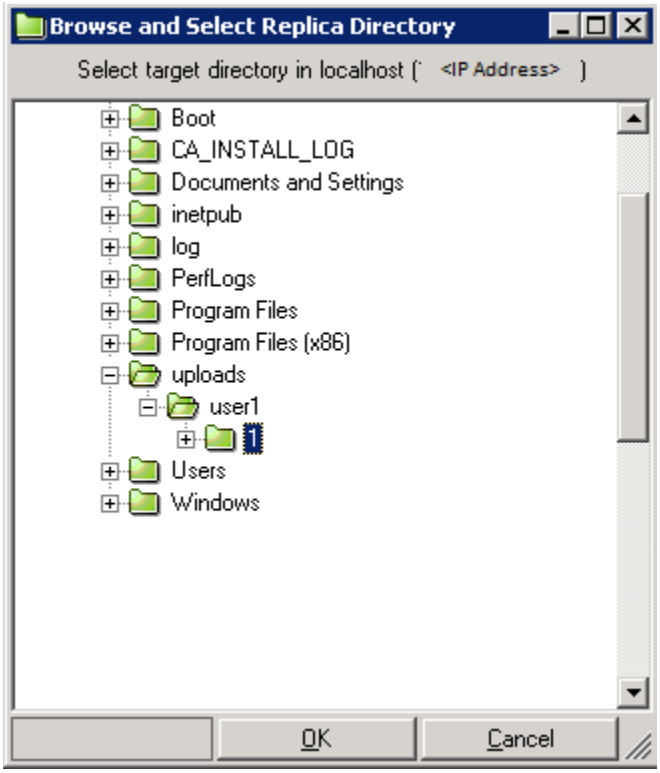
1. Accedere al server di replica e alla cartella dove sono state create le cartelle utente.
2. Fare clic con il tasto destro del mouse su una cartella utente e fare clic su Proprietà.
3. Selezionare la scheda Protezione.
4. Selezionare l'utente e concedere le autorizzazioni di controllo completo.



Allo stesso modo, selezionare altre cartelle utente e concedere le autorizzazioni di controllo completo.

Creazione ed esecuzione dello scenario (Utenti)

Durante la creazione dello scenario, immettere le credenziali di replica valide e selezionare la cartella principale nella cartella padre specificata. Le credenziale utente e i dettagli di cartella vengono forniti all'utente dell'amministratore MSP.



Durante l'esecuzione dello scenario, RHA verifica le condizioni seguenti:

1. Credenziali a livello di scenario per ciascun host.
2. Credenziali a livello di host per ciascun host. Le credenziali a livello di host sovrascrivono le credenziali a livello di scenario. Se le credenziali a livello di host sono vuote o non vengono impostate, RHA utilizza automaticamente le credenziali a livello di scenario.
3. L'utente dispone delle autorizzazioni di controllo completo per la cartella padre specificata.

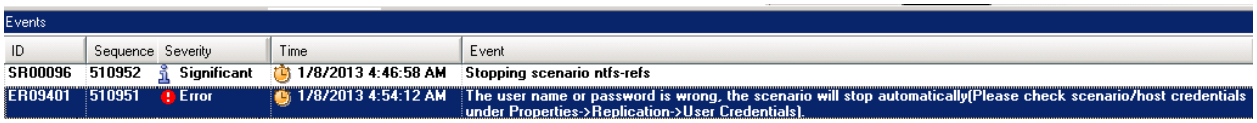
Lo scenario viene eseguito correttamente solo se le credenziali host e le autorizzazioni di accesso alla cartella vengono convalidate. Se una di queste condizioni non si verifica, lo scenario viene interrotto immediatamente. Correggere lo scenario con le credenziali corrette o con la cartella di replica valida.

Verifica degli eventi (Utenti)

Nel caso in cui le credenziali host specificate non siano valide o l'utente non disponga delle autorizzazioni di controllo completo per la cartella padre, si verifica un errore di esecuzione dello scenario. Se non è possibile eseguire lo scenario, Arcserve RHA visualizza un errore. Verificare l'errore e modificare lo scenario.

Correzione ed esecuzione dello scenario (Utenti)

Se si verifica un errore dello scenario e Arcserve RHA visualizza un errore, modificare lo scenario e verificare le credenziali di replica o la cartella di replica.



Procedere come descritto di seguito:

1. Accedere a Gestione di CA ARCserve RHA e selezionare lo scenario.
2. Dalla visualizzazione Scenario, selezionare il server di replica e fare clic su Proprietà nel riquadro di destra.
3. Espandere Replica e fare clic su Credenziali utente.

Specificare le credenziali corrette per il server di replica e selezionare la directory principale della cartella padre fornita dall'amministratore.

Disattivazione dell'autenticazione

Per impostazione predefinita, il parametro EnableAuth del file ws_rep.cfg viene impostato su True. Per disattivare l'autenticazione host su un host specifico, impostare il parametro EnableAuth nel file ws_rep.cfg su False.

Procedere come descritto di seguito:

1. Aprire ws_rep.cfg.
2. Modificare il parametro EnableAuth su False.

L'autenticazione host viene disabilitata.

Considerazioni e limiti

Tenere presenti le seguenti considerazioni e limiti della replica multitenancy:

- Gli amministratori locali o di dominio possono eseguire correttamente gli scenari, incluso nel caso in cui non dispongano delle autorizzazioni specifiche per le cartelle di replica.
- Durante la creazione di uno scenario, gli utenti possono visualizzare la struttura di directory di altri utenti.
- Solo agli amministratori sono in grado eseguire gli script di scenario per impostazione predefinita. Per consentire ad altri utenti di eseguire lo script, impostare OnlyAdminCanRunScript in ws_rep.cfg su False.

Chiusura e apertura della Gestione durante la replica

Dopo aver definito lo scenario e avviato la replica, è possibile chiudere la Gestione. È possibile lasciarla aperta solo per il monitoraggio in tempo reale del processo di replica. La chiusura della Gestione NON implica l'interruzione degli scenari in esecuzione. Alla riapertura, verranno caricati automaticamente tutti gli scenari salvati, il cui stato verrà visualizzato.

Nota: anche quando la Gestione è chiusa, è possibile monitorare il sistema replicato tramite la Pagina con informazioni introduttive. È anche possibile ricevere notifiche tramite posta elettronica oppure eseguendo automaticamente script definiti dall'utente quando si verificano eventi importanti o degli errori Per ulteriori informazioni, consultare le sezioni relative alla *notifica eventi* in*Proprietà scenario, server master e di replica*.

Sospendi replica

A volte può essere necessario sospendere gli aggiornamenti sul computer di replica per eseguire la manutenzione del sistema o altri tipi di elaborazione che non modificano i dati replicati. Di solito, non è auspicabile interrompere la replica, in quanto essa richiede in seguito una completa risincronizzazione. La funzionalità di sospensione della replica di Arcserve RHA consente di risolvere questo problema.

Durante il periodo di sospensione, tutte le modifiche vengono inserite nello spool sul server master o sul server di replica situato a monte del server di replica sospeso. In altri termini, la registrazione delle modifiche continuerà a essere eseguita per l'aggiornamento del server di replica sospeso, ma il trasferimento effettivo non verrà eseguito fino alla ripresa della replica. Quando la replica viene ripresa, le modifiche accumulate vengono trasferite e applicate senza necessità di eseguire una risincronizzazione completa dei dati.

La replica può essere sospesa manualmente o su base pianificata.

Importante: durante la sospensione, è indispensabile che l'utente non esegua sul server di replica operazioni che possano in qualsiasi modo causare la modifica dei dati, tra cui l'avvio di applicazioni quali Exchange Server, SQL Server o Oracle. Se è necessario avviare programmi che modificano i dati sul server di replica, utilizzare l'opzione Assured Recovery (a pagina 309).

Prestare attenzione a quanto esposto di seguito:

- Non è possibile sospendere la replica durante la sincronizzazione. È possibile sospendere la replica solo temporaneamente, dal momento che le modifiche vengono accumulate nella directory di spool del server master o del server di replica a monte. Assicurarsi che sia disponibile spazio su disco sufficiente affinché lo spool possa contenere le modifiche apportate durante la sospensione del server di replica.
- In uno scenario con più di un host di replica, è possibile sospendere solo un server di replica alla volta.

Sospensione manuale della replica

È possibile sospendere manualmente la replica per operazioni di manutenzione del sistema.

Per procedere alla sospensione manuale della replica:

1. Dalla Gestione, selezionare la replica che si desidera sospendere. Quindi, fare clic su Sospendi oppure selezionare l'opzione di sospensione replica dal menu Strumenti.

   Viene visualizzato un messaggio di conferma, in cui l'utente viene informato che le eventuali modifiche apportate al contenuto delle directory principali di replica durante la sospensione richiederanno la risincronizzazione manuale.

2. Fare clic su **Sì** per sospendere la replica.

   Dopo aver sospeso la replica, verrà visualizzata un'icona di colore rosso accanto alla replica nel riquadro Scenario.

   Nota:durante la sospensione, lo stato dello scenario non cambia ma rimane **In esecuzione**, dal momento che è stata sospesa solo la replica sul server di replica.

   Nel riquadro Statistiche scenario, viene visualizzata un'icona di sospensione con una didascalia che informa che la replica è stata sospesa.

3. Durante la sospensione della replica è possibile eseguire interventi di manutenzione sul server di replica, incluso il riavvio di tale server. Tuttavia, è di estrema importanza non modificare i dati replicati in alcun modo, altrimenti sarà necessario eseguire una risincronizzazione con il server master.

   Nota: è possibile eseguire un comando di sincronizzazione quando un server di replica è sospeso. Tuttavia, esso verrà eseguito solo dopo la ripresa della replica.

Ripresa della replica in seguito a una sospensione manuale

Durante la sospensione della replica, le modifiche vengono mantenute in uno spool sul master. Dopo aver completato le operazioni di manutenzione del sistema, sarà necessario riprendere la replica e terminare il periodo di sospensione manuale. Le modifiche accumulate sul server master verranno, quindi, trasferite sul server di replica.

Per riprendere la replica in seguito a una sospensione manuale, procedere come segue:

1. Dopo aver sospeso un server di replica, il pulsante **Sospendi** sulla barra degli strumenti della Gestione cambia in Resume replication (Riprendi replica). Per riprendere la replica, fare clic sul pulsante Resume replication (Riprendi replica) oppure selezionare l'opzione dal menu Strumenti.

   Verrà visualizzato un messaggio di conferma.

2. Fare clic su **Sì** per riprendere la replica.

   Dopo aver ripreso la replica, l'icona di colore rosso non viene più visualizzata accanto alla replica nel riquadro Scenario e il simbolo di sospensione scompare dal riquadro Statistiche scenario.

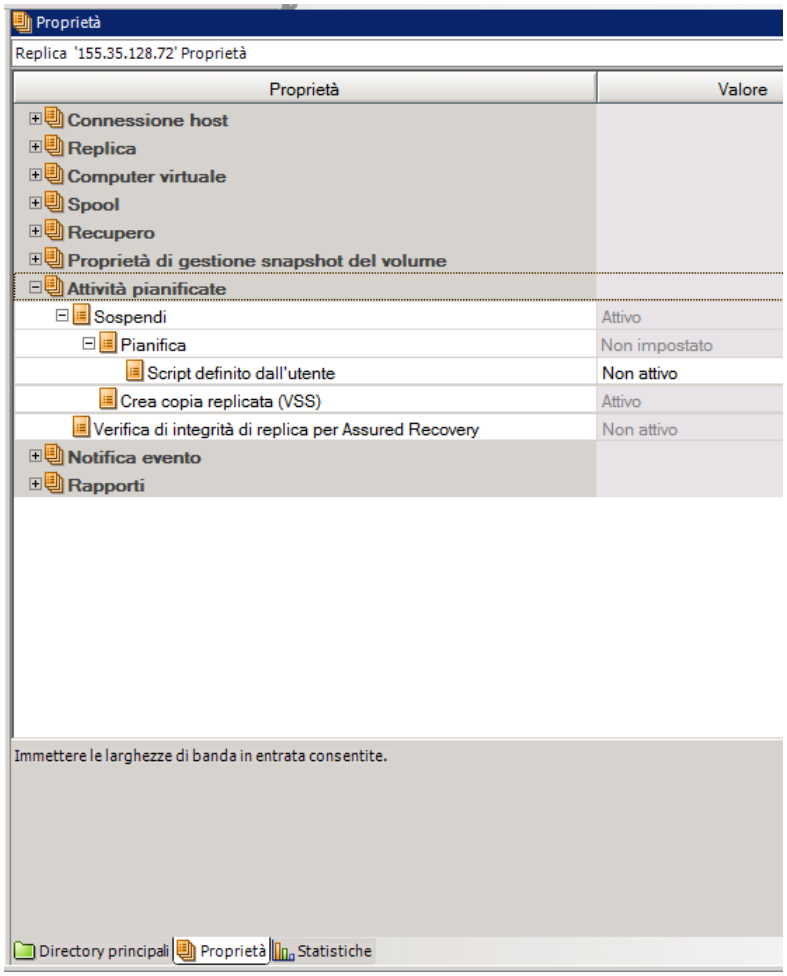
Pianificazione della sospensione replica automatica

È possibile pianificare la sospensione automatica della replica.

Per pianificare la sospensione automatica della replica, procedere come segue:

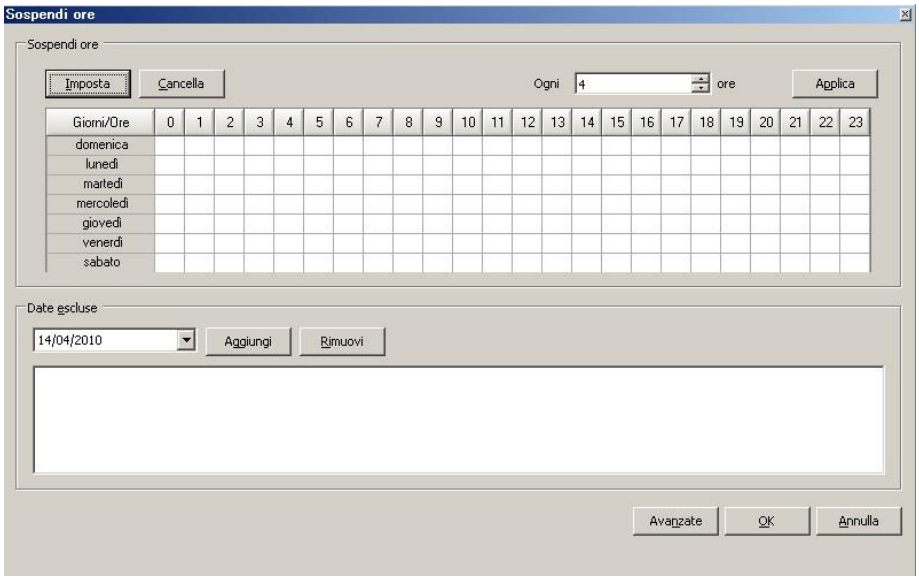
1. Dalla Gestione, selezionare il server di replica che si desidera sospendere e interrompere lo scenario del quale fa parte.
2. Nel riquadro Struttura, selezionare la scheda Proprietà per aprire l'elenco Proprietà server di replica.

3. Nell'elenco Proprietà di replica, aprire il gruppo Attività pianificate. Nella proprietà Sospensione, impostare il valore su Attivo.



4. Nella proprietà Pianificazione, fare clic sulla casella di valore.

   Viene visualizzata la finestra di dialogo Sospendi ore.



   La finestra di dialogo Sospendi ore è simile alla finestra di dialogo Impostazioni di pianificazione, utilizzata per pianificare la sincronizzazione automatica. Per informazioni sull'impostazione di una pianificazione, fare riferimento all'argomento Pianificazione della sincronizzazione (a pagina 211).

5. Impostare la sospensione automatica del piano nella finestra di dialogo Sospendi ore. Fare clic su OK per salvare il piano e chiudere la finestra.

6. Per attivare la pianificazione, fare clic sul pulsante Salva nella barra degli strumenti standard e avviare lo scenario.

   Il server di replica selezionato per la sospensione verrà sospeso e ripreso in base al piano impostato.

Esecuzione di uno scenario in modalità di valutazione

Arcserve RHA consente di eseguire uno scenario senza in realtà replicare dati, per valutare accuratamente la larghezza di banda utilizzata e il benchmarking del rapporto di compressione necessario per la replica. Quando uno scenario viene eseguito in modalità valutazione, non viene eseguita alcuna replica, ma vengono raccolti dati statistici. Una volta interrotto il processo di valutazione, verrà stilato un rapporto.

Per utilizzare l'opzione di modalità di valutazione, è necessario creare un nuovo scenario e selezionare la casella di controllo **Modalità valutazione** nella Creazione guidata scenario.

Uno scenario eseguibile in modalità di valutazione può essere eseguito anche in modalità di replica normale. Quando viene inizializzato lo scenario, il pulsante selezionato, a seconda che si tratti del pulsante verde **Esegui** o del pulsante blu **Esegui (Modalità valutazione)**, determina la modalità di esecuzione dello scenario.

Per eseguire uno scenario in Modalità valutazione:

1. Dalla Gestione, selezionare lo scenario che si desidera eseguire in modalità di valutazione.

2. Per eseguire lo scenario, fare clic sul pulsante **Esegui (Modalità valutazione)** sulla barra degli strumenti standard.

   Arcserve RHA verifica lo scenario prima di procedere all'esecuzione.

3. Se lo scenario non è stato impostato correttamente oppure si sono verificati dei problemi negli host presenti, gli errori verranno segnalati nel riquadro Eventi. Quando non viene segnalato alcun errore, l'esecuzione dello scenario ha inizio.

   La Gestione indica, quindi, che lo scenario è in esecuzione in Modalità di valutazione tramite il simbolo di riproduzione di colore blu posto a sinistra dello scenario e lo stato dello scenario, che diventa **Simulazione**.

4. Quando lo scenario è in esecuzione, alla base del riquadro Struttura viene visualizzata la scheda Statistiche, che contiene una rappresentazione grafica della valutazione della replica.

5. Per impostazione predefinita, dopo aver interrotto uno scenario eseguito in modalità di valutazione, viene generato un Rapporto modalità valutazione (a pagina 170). Per aprire il rapporto, si rimanda alla sezione Visualizzazione di un rapporto (a pagina 167).

Capitolo 6: Monitoraggio della replica

In questa sezione viene fornita una descrizione dei diversi strumenti di monitoraggio di Arcserve RHA che consentono di controllare e monitorare il proprio ambiente di replica.

Questa sezione contiene i seguenti argomenti:

Pagina con informazioni introduttive (a pagina 155)
Gestione (a pagina 155)
Visualizzazione eventi (a pagina 164)
Rapporti di Arcserve RHA (a pagina 166)

Pagina con informazioni introduttive

La Pagina con informazioni introduttive consente di eseguire il monitoraggio simultaneo da parte di un numero qualsiasi di amministratori o professionisti che desiderano essere informati sullo stato del sistema replicato.

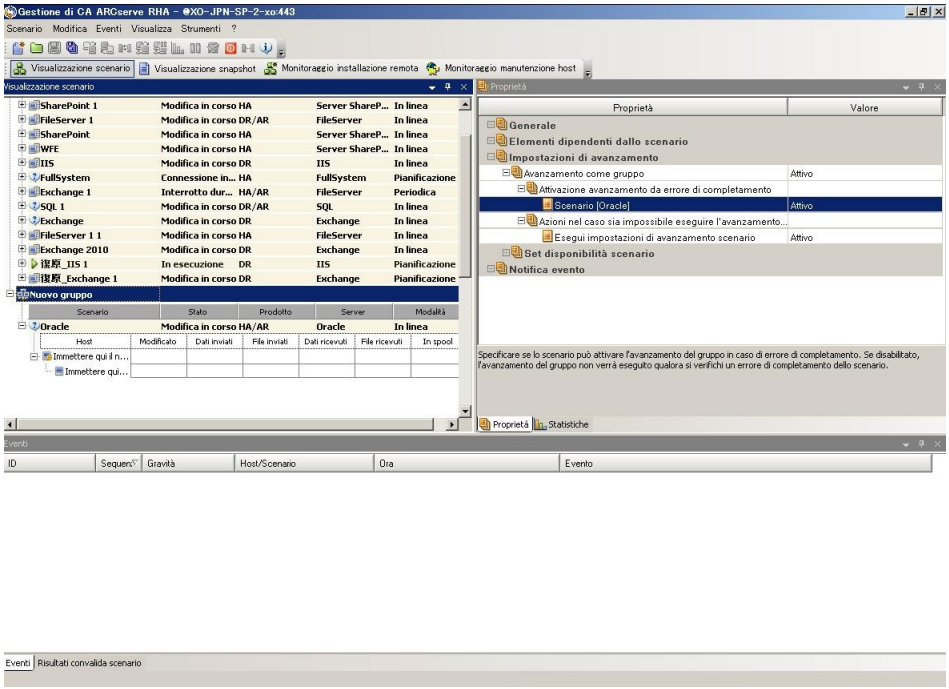
Nota: non è necessario aggiornare il browser; la Pagina con informazioni introduttive si aggiorna automaticamente.

Gestione

La Gestione consente di controllare e monitorare il sistema replicato.

Modalità di controllo per scenari multipli

Il riquadro Scenario mostra lo stato corrente di tutti gli scenari in un singolo riquadro.



È possibile personalizzare la modalità di visualizzazione delle colonne. Per ulteriori informazioni, consultare la sezione Personalizzazione della visualizzazione scenario (a pagina 37).

Informazioni sullo stato

Le informazioni sullo stato vengono visualizzate accanto al nome di ogni scenario e accanto ad ogni server nella struttura di replica, ogni volta che viene avviato o completato un processo di sincronizzazione o è in corso un processo di replica.

Le informazioni di stato includono:

- Un'indicazione grafica accanto al nome dello scenario, indicante che lo scenario è in esecuzione o inattivo .
- Un'indicazione grafica accanto al nome del server, indicante che il server è un server master (attivo) o un server di replica (in stand-by) .
- Un'indicazione grafica che mostra se il server è connesso: se la connessione a uno dei server partecipanti viene persa, l'icona del server viene contrassegnata con una grande **X** di colore rosso.

Statistiche live

Le statistiche live sono visualizzare in due aree:

- Riquadro Scenario
- Riquadro Statistiche

Riquadro Scenario

Le statistiche live visualizzate nel riquadro Scenario includono le seguenti informazioni:

- **Modificato**: numero totale dei dati replicati da questo host a partire dall'ultima sincronizzazione.
- **Sincronizzato**: numero totale dei dati sincronizzati da questo host.
- **File**: numero totale di file replicati da questo host.
- **In spool**: quantità totale (corrente) dei dati contenuti nello spool.

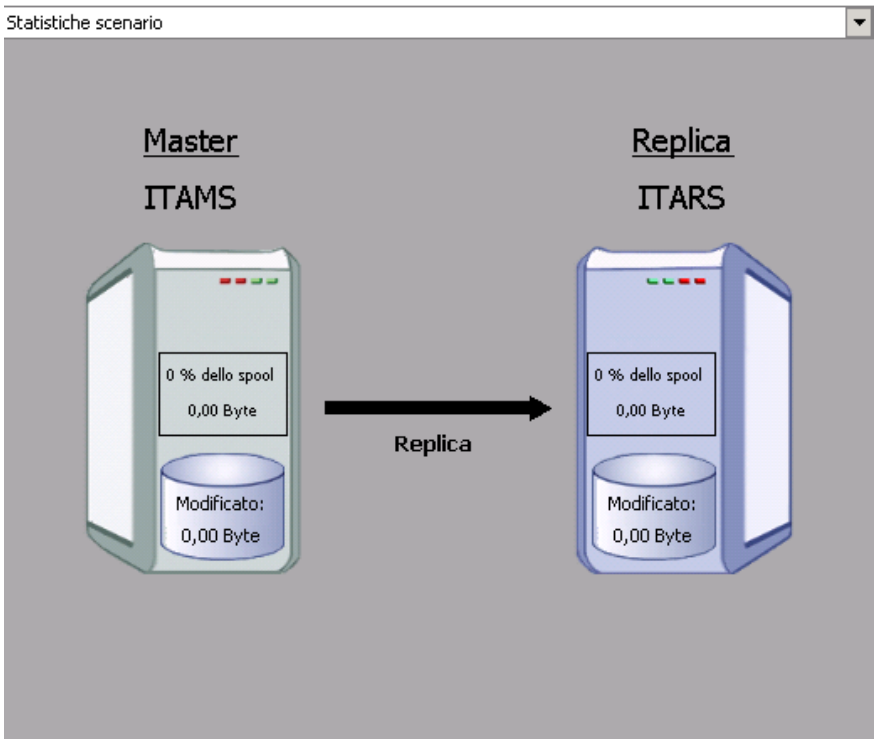
Scheda Statistiche.

La scheda Statistiche nel riquadro Struttura contiene anche le statistiche live. Vengono visualizzati diversi dati statistici per uno scenario, un server master e ogni server di replica.

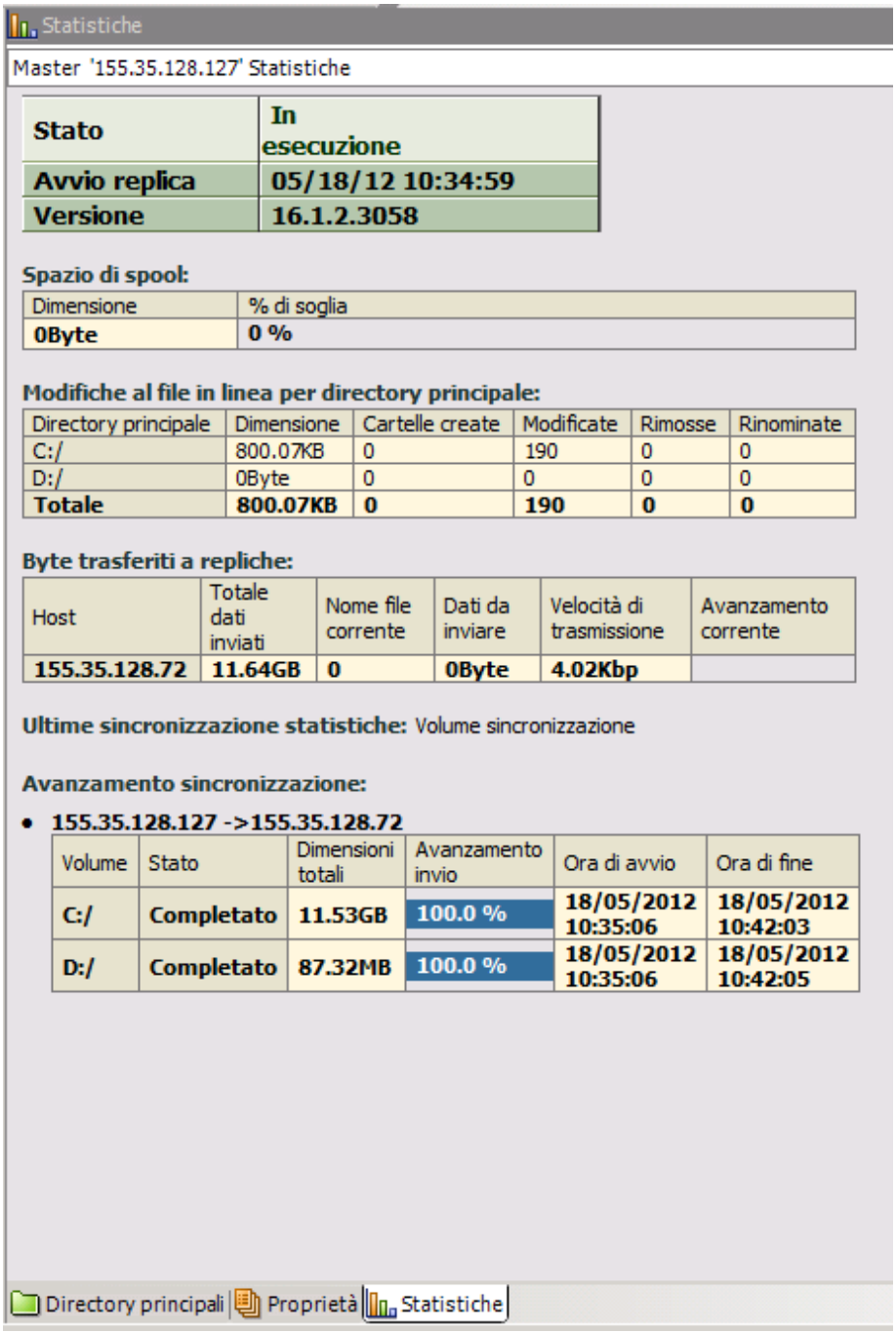
Nota: la scheda Statistiche nel riquadro Struttura è visibile solo quando uno scenario è in esecuzione.

Di seguito sono elencate le informazioni live disponibili nella scheda Statistiche:

- **Statistiche per scenario**: una panoramica grafica dello stato dello scenario.



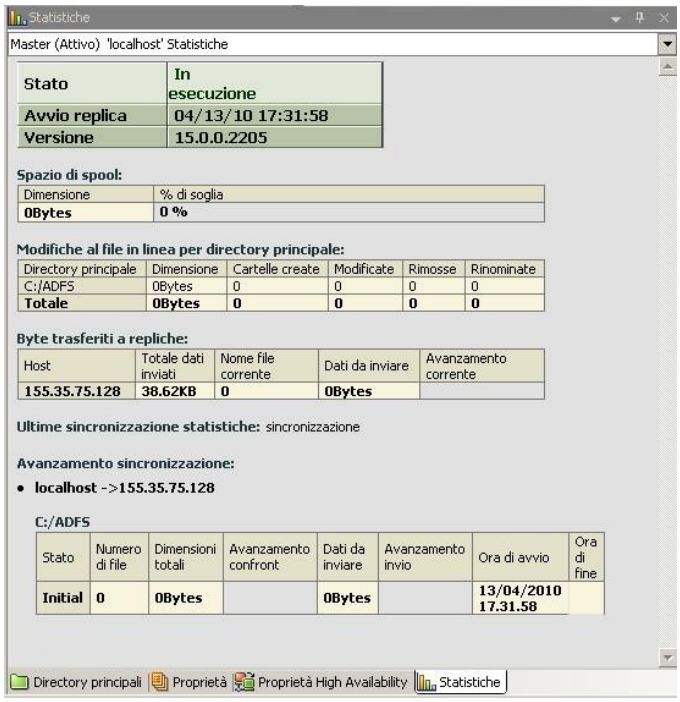
- **Statistiche per server master**: tabella contenente le seguenti informazioni: stato, data e ora di avvio della replica; numero di versione del Modulo Arcserve RHA; quantità totale di dati contenuti nello spool; quantità totale di dati modificati nelle directory principali dall'inizio del processo di replica, incluso il numero di cartelle create e modificate e di file rimossi e rinominati; dimensione totale dei file inviati e replicati dall'host; metodo di sincronizzazione e avanzamento della sincronizzazione.



Quando si esegue la sincronizzazione per file di grandi dimensioni, vengono visualizzate tabelle aggiuntive che mostrano i dettagli dell'avanzamento della sincronizzazione per ciascun file in ciascuna directory principale.

Prestare attenzione a quanto esposto di seguito:

- La definizione di un file di grandi dimensioni dipende dal valore della proprietà BDMaxFileSizeToSendWholly. Questa proprietà è archiviata nel computer su cui è installato il modulo, nel file INSTALLDIR\Engine\ws_rep.cfg. Il valore predefinito è 10 MB. I file sincronizzati di dimensioni inferiori, non saranno riportati nella tabella.
- L'aspetto della tabella dettagliata Stato sincronizzazione dipende inoltre dal valore della proprietà UseNewSynchStatistics. Questa proprietà determina la visualizzazione della tabella dettagliata Stato sincronizzazione in presenza di file di grandi dimensioni. Se il valore di questa proprietà è True, viene visualizzata la tabella. Il valore predefinito è True e la proprietà è archiviata nel file ws_rep.cfg.

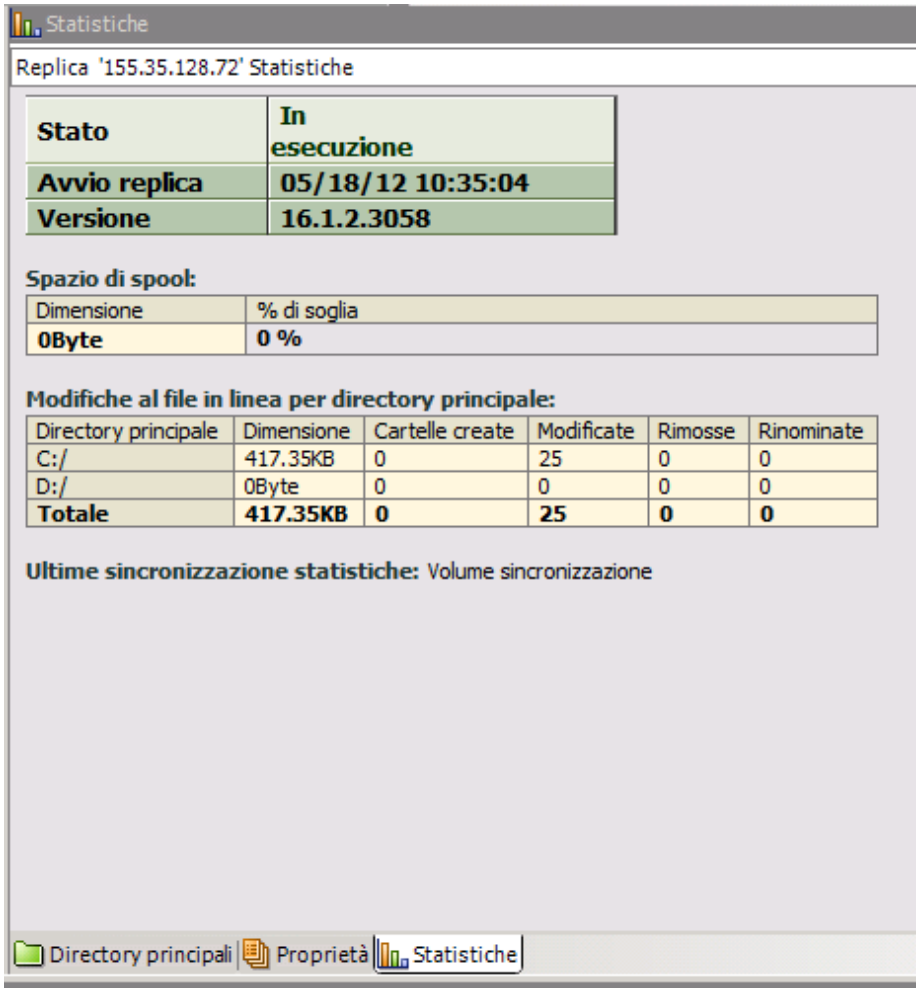


Le tabelle Stato sincronizzazione contengono le seguenti informazioni per ciascun file sincronizzato: stato della sincronizzazione, nome del file, dimensioni del file, quantità e percentuale dei dati già confrontati tra server master e server di replica, quantità dei dati da inviare dal server master al server di replica, quantità e percentuale dei dati identici tra server master e server di replica (quindi non inviati al server di replica), data e ora di inizio della sincronizzazione, riepilogo dello stato di avanzamento della sincronizzazione per ciascuna directory principale.

Nota: se è in esecuzione il metodo Sincronizzazione file, i file vengono sincronizzati interamente. Di conseguenza, la colonna Già verificato potrebbe contenere solo due valori: 0% o 100%, per ciascun file.

Ciascuna directory principale sincronizzata è rappresentata in una tabella Stato sincronizzazione distinta e ciascuna tabelle mostra le statistiche per un massimo di 10 file. Se una directory principale contiene più di 10 file, la tabella includerà i 10 file di dimensioni maggiori.

- **Statistiche per server di replica**: tabella contenente le seguenti informazioni: stato e data dell'avvio della replica; numero della versione di Arcserve RHA; quantità totale di dati contenuti nello spool; quantità totale di dati (in KB) modificati nelle directory principali dall'inizio del processo di replica, incluso il numero di file modificati, rimossi e rinominati.



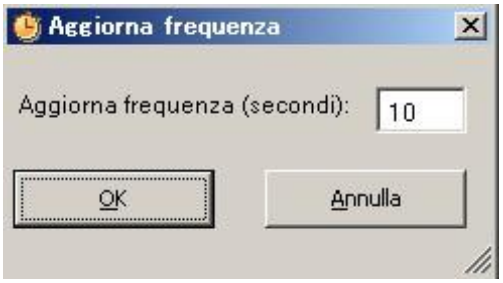
Aggiornamento automatico della visualizzazione di statistiche

La Gestione riceve le informazioni di stato da tutti i server facenti parte dello scenario corrente. È possibile impostare una frequenza predefinita per l'aggiornamento automatico della visualizzazione di informazioni di stato e statistiche live.

Per definire la frequenza di aggiornamento, procedere come segue:

1. Dal menu Strumenti, selezionare Statistiche, Aggiorna frequenza.

   Viene visualizzata la finestra di dialogo Aggiorna frequenza.



2. Immettere la frequenza di aggiornamento in secondi desiderata e fare clic OK. Il riquadro Scenario verrà aggiornato di conseguenza.

   Nota: l'intervallo della frequenza di aggiornamento può essere compreso tra 10 e 99 secondi.

Consultare la sezione Aggiornamento manuale della visualizzazione di statistiche

Per aggiornare manualmente le informazioni visualizzate, procedere come segue:

1. Fare clic su Aggiorna statistiche sulla barra degli strumenti standard della schermata di Gestione.
2. Premere il tasto F5.
3. Dal menu Strumenti, selezionare Statistiche, Aggiorna.

   I dati relativi alle statistiche verranno aggiornati.

Visualizzazione eventi

Nel riquadro Eventi sono visualizzati messaggi e informazioni generali sullo scenario selezionato. Queste informazioni vengono ricevute dai server che appartengono allo scenario in esecuzione. Le informazioni visualizzate possono informare l'utente, ad esempio, che la sincronizzazione di una directory è stata completata, che un server è connesso, che la sincronizzazione è stata avviata/terminata, e così via. Le informazioni includono il nome server, il tempo e una breve spiegazione. Eventi importanti o messaggi di errore sono visualizzati in grassetto.

Visualizzazione di eventi in una finestra separata

Talvolta, alcuni messaggi di eventi sono molti lunghi e oltrepassano l'area degli eventi, e pertanto vengono troncati (visivamente). In questi casi, può essere opportuno visualizzare i messaggi di evento in finestre separate.

Per visualizzare eventi in una finestra separata:

1. Dal riquadro di gestione eventi, selezionare l'evento che si desidera visualizzare.
2. Fare doppio clic sull'evento oppure fare clic su di esso con il pulsante destro del mouse e selezionare Visualizza evento in un'altra finestra dal menu di scelta rapida. In alternativa, selezionare l'opzione Visualizza evento in un'altra finestra dal menu Eventi.

   Viene visualizzato un messaggio con il testo completo del messaggio relativo all'evento selezionato.

Visualizzazione di eventi in entrata

La Gestione può inviare una notifica all'utente in caso di eventi in entrata.

Per visualizzare gli eventi in entrata quando si verificano

1. Dal menu di gestione eventi, selezionare l'opzione Popup evento in entrata.

   Quando un evento è in entrata, l'icona della Gestione lampeggia nella barra delle attività e la Gestione viene portata in primo piano.

   Nota: se si seleziona di nuovo quest'opzione e la si disattiva, l'applicazione ridotta a icona nella barra delle applicazioni non lampeggia quando è in arrivo un evento.

Copia di eventi per l'utilizzo con altri programmi

Quando si verificano eventi importanti, l'utente potrebbe desiderare copiare i relativi messaggi su altri programmi.

Per copiare eventi ed utilizzarli con altri programmi:

1. Nel riquadro Eventi, selezionare un numero qualsiasi di eventi mediante il tasto CTRL.
2. Fare clic con il pulsante destro del mouse sul riquadro Eventi e selezionare Copia, oppure selezionare l'opzione Copia nel menu Eventi. In alternativa, premere CTRL+C.

   È possibile incollare i testi dell'evento copiati in qualsiasi programma desiderato.

   Nota: Arcserve RHA consente, inoltre, di copiare il messaggio di evento direttamente in un file con estensione CSV, ad esempio i file Excel. Dopo aver selezionato l'opzione di copia in CSV , verrà aperta l'applicazione definita sul proprio computer come CSV, visualizzando il messaggio copiato (per impostare l'applicazione CSV predefinita, consultare la sezione Risorse del computer, Strumenti, Opzioni cartella, Tipi di file, CSV).

Filtro eventi

È possibile filtrare gli eventi da visualizzare nel riquadro Evento in base a diversi criteri.

Per filtrare gli eventi visualizzati, procedere come segue:

1. Nel riquadro Evento, fare clic con il pulsante destro del mouse e scegliere Filtri evento dal menu di scelta rapida oppure scegliere l'opzione Filtri evento dal menu Eventi.

   Viene visualizzata la finestra Filtri evento.

2. Utilizzare uno dei seguenti criteri per filtrare gli eventi visualizzati nel riquadro Evento:
   - **Gravità**: deselezionare le caselle di controllo relative al livello di gravità che non si desidera visualizzare oppure selezionare quelle che si desidera visualizzare.
   - **Data**: selezionare la casella di controllo Escludi eventi precedenti a, quindi l'unità di tempo (ore/giorni/mesi) e il relativo numero di unità.
   - **Testo**: nella casella Una parola o una frase in questo evento, immettere la parola o la frase che gli eventi da visualizzare dovranno contenere. È possibile utilizzare un asterisco (*) per selezionare un numero qualsiasi di caratteri/cifre di tutti i tipi.
3. Per applicare i criteri selezionati e chiudere la finestra di dialogo, fare clic su OK.

   Nel riquadro Evento, saranno ora visualizzati solo gli eventi che soddisfano i criteri definiti.
4. Per deselezionare i criteri esistenti e visualizzare tutti gli eventi, fare clic sul pulsante Ripristina nella finestra di dialogo Filtri evento, quindi su OK.

Rapporti di Arcserve RHA

Arcserve RHA è in grado di generare rapporti sui processi di replica e sincronizzazione. Questi rapporti possono essere memorizzati nella posizione desiderata, aperti per la visualizzazione dal Report Center, inviati per posta elettronica a un indirizzo specificato, oppure possono attivare l'esecuzione di script. Per impostare queste opzioni, vedere quanto segue.

- Per la definizione della directory di archiviazione e del periodo di conservazione dei rapporti, si rimanda alla sezione Nozioni fondamentali sulle proprietà dello scenario (a pagina 202).
- Per la definizione della generazione automatica dei rapporti di sincronizzazione e di replica per il server master, si rimanda alla sezione Nozioni fondamentali sulle proprietà del server master (a pagina 217).
- Per la definizione della generazione automatica dei rapporti di replica per il server di replica, si rimanda alla sezione Nozioni fondamentali sulle proprietà del server di replica (a pagina 224).

Per impostazione predefinita, Arcserve RHA memorizza i rapporti nella seguente directory: *[Cartella Programmi] \CA\Arcserve RHA\Manager\reports*

Importante: Non è possibile creare un rapporto se il nome dello scenario contiene caratteri speciali (\/?:"<>|,).

Visualizzazione di un rapporto

I rapporti di Arcserve RHA consentono di determinare lo stato dello scenario e di gestire l'ambiente.

Per visualizzare un rapporto, procedere come segue:

1. Per visualizzare un rapporto è innanzitutto necessario aprire il Report Center. A questo scopo, si possono utilizzare due metodi:

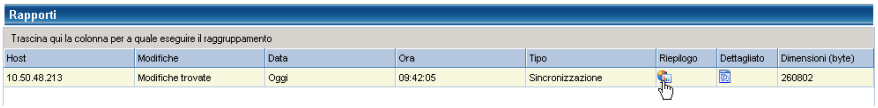
   - Nella Pagina con informazioni introduttive, fare clic sul collegamento Report Center nel riquadro Avvio rapido a sinistra:
   - Nel menu Strumenti, selezionare Rapporti, quindi Show Scenario Reports (Visualizza rapporti scenario).

   Il Report Center viene aperto all'interno di una nuova finestra.

   Il Report Center è costituito da due tabelle:

   - La tabella superiore, denominata Rapporti disponibili per scenario, contiene un elenco di tutti gli scenari con rapporti, oltre al tipo e al numero di rapporti disponibili per ogni scenario.
   - La tabella inferiore, denominata Rapporti, contiene un elenco di tutti i rapporti disponibili per lo scenario selezionato nella tabella superiore.

2. Per visualizzare un rapporto specifico, nella tabella Rapporti disponibili per scenario selezionare lo scenario rappresentato da questo rapporto. Quindi, nella tabella Rapporti sottostante, fare clic sul rapporto che si desidera visualizzare.



   Nota: a seconda delle impostazioni dell'utente, oltre al rapporto di riepilogo, è possibile generare un rapporto dettagliato per i rapporti di sincronizzazione e di replica. Entrambi i rapporti rappresentano lo stesso processo, ma il rapporto dettagliato fornisce inoltre un elenco dei file presenti nel processo.

   Viene visualizzato il rapporto selezionato.

Eliminazione di rapporti

I rapporti che vengono visualizzati nel Report Center vengono memorizzati per il periodo definito nelle proprietà dei relativi scenari nel gruppo Gestione dei rapporti (a pagina 210). I rapporti vengono visualizzati anche se i relativi scenari sono stati rimossi dalla Gestione. Tuttavia, nel Report Center è possibile eliminare i rapporti che non sono più di nessuna utilità.

Per eliminare un rapporto

1. Nel Report Center, dalla tabella Rapporti disponibili per scenario selezionare lo scenario i cui rapporti si intende eliminare.
2. Fare clic su Elimina all'estremità destra della linea.

   Viene visualizzato un messaggio di conferma dell'eliminazione della riga.
3. Fare clic su OK nel messaggio di conferma.

   Lo scenario selezionato verrà rimosso dal Report Center e tutti i rapporti ad esso appartenenti verranno eliminati.

Rapporti di sincronizzazione

Dopo la sincronizzazione, Arcserve RHA crea un rapporto che elenca i file trasferiti o modificati. Le prime linee (in alto) includono: il metodo di sincronizzazione, il nome dello scenario, i nomi dei server master e di replica e la data di sincronizzazione.

Nel riepilogo del rapporto di sincronizzazione è illustrata la somma totale dei file rimossi e modificati, nonché dei byte trasferiti. Il rapporto fornisce inoltre informazioni sul numero di nuove directory create sul server di replica in seguito alla sincronizzazione e sul numero di file sincronizzati con diverse proprietà di protezione Windows.

Il Rapporto di sincronizzazione dettagliato presenta l'elenco completo dei file che sono stati trasferiti o modificati durante il processo di sincronizzazione. Per ogni file, vengono fornite le informazioni elencate di seguito:

- **Evento**: l'operazione eseguita sul server di replica.
- **Byte**: la dimensione del file.
- **Timestamp**: l'ora della modifica.
- **Nome file**: il nome e il percorso completo del file.

Rapporti di replica

I rapporti di replica vengono generati periodicamente, in base a una frequenza predefinita, e individualmente per i server master e di replica.

I rapporti di replica includono statistiche sui dati replicati dall'inizio del processo, nonché statistiche sui dati replicati dall'ultimo rapporto. I dati includono il numero di byte replicati e il numero di file creati/aggiornati/rimossi e rinominati. È possibile visualizzare un rapporto sintetico o dettagliato.

Per impostazione predefinita i rapporti di replica NON vengono generati automaticamente. Per pianificare rapporti di replica, consultare la sezione Proprietà rapporti. (a pagina 222)

Per aprire un rapporto su uno scenario precedente, procedere come segue:

Un rapporto su scenario precedente è in effetti un rapporto di sincronizzazione, che mostra le informazioni di sincronizzazione relative a uno scenario precedente.

Per aprire un rapporto su scenario precedente, procedere come segue:

1. Nel Report Center, selezionare lo scenario precedente dalla tabella Rapporti disponibili per scenario.
2. Nella tabella Rapporti, selezionare il rapporto di sincronizzazione che si intende visualizzare.
3. Viene visualizzato il rapporto di sincronizzazione per lo scenario precedente.

Rapporti delle differenze

Un rapporto delle differenze confronta le differenze fra il master e la replica in un determinato momento. Il confronto viene eseguito mediante gli stessi algoritmi utilizzati nel processo di sincronizzazione, ma senza trasferire alcun dato. Per ogni server di replica verrà generato un rapporto delle differenze, che verrà quindi inviato alla Gestione al termine del processo. Il rapporto delle differenze può essere generato in qualsiasi momento.

Nota: quando si procede all'esecuzione di un rapporto delle differenze su una piattaforma SQL Server 2008/Windows Server 2008 R2, le differenze vengono segnalate in base al modo in cui SQL Server 2008 prealloca la dimensione di buffer. Questa differenza non influisce sull'integrità del database.

Importante: si sconsiglia di avviare un rapporto delle differenze quando è in corso l'aggiornamento dei dati sul server master, in quanto tutti gli aggiornamenti non ancora applicati al server di replica verranno indicati come differenze.

Per creare rapporti delle differenze:

1. Fare clic sull'icona Rapporto delle differenze nella barra degli strumenti standard oppure selezionare l'opzione Rapporto, Rapporto delle differenze dal menu Strumenti.

   Viene visualizzata la finestra di dialogo Rapporto delle differenze con gli stessi metodi di confronto della finestra di dialogo Metodo di sincronizzazione.

2. Scegliere le opzioni desiderate, seguendo le istruzioni specificate nella sezione Funzionamento della sincronizzazione *(a pagina 18).*

3. Fare clic su OK.

   Al termine del processo, per ogni server di replica verrà generato un rapporto delle differenze; tutti i rapporti generati verranno successivamente inviati al Report Center.

Rapporti della modalità valutazione

Arcserve RHA genera rapporti della modalità valutazione a seguito dell'interruzione di scenari in esecuzione in modalità valutazione. Tale rapporto visualizza le statistiche relative al totale dei byte previsti per il trasferimento dal master alla replica, dall'inizializzazione dello scenario alla sua interruzione.

La somma totale dei byte previsti per il trasferimento viene calcolata per unità di tempo predefinite, denominate "timestamp". Per impostazione predefinita, un timestamp viene calcolato ogni 10 minuti.

Nota: è possibile modificare l'intervallo di timestamp predefinito nel file **ws_rep.cfg**, immettendo un nuovo valore per il parametro **AssessmentTimeSample**.

La tabella **Riepilogo** del Rapporto modalità valutazione mostra le statistiche relative alla dimensione massima, minima e media dei dati previsti per il trasferimento durante l'esecuzione dello scenario. Fornisce anche statistiche sui dati previsti per il trasferimento in formato compresso.

Capitolo 7: Modifica e gestione di scenari e host

Questa sezione illustra la configurazione manuale di uno scenario di replica file server e il processo di rilevamento automatico per le applicazioni di database. Per ulteriori istruzioni sugli scenari personalizzati per applicazioni specifiche quali Exchange Server o SQL Server, si rimanda alla Guida operativa appropriata.

Dopo aver creato uno scenario utilizzando la Creazione guidata scenario, sarà possibile modificare manualmente la maggior parte delle definizioni. Sebbene non sia possibile procedere alla creazione manuale di uno scenario da zero, è possibile fare clic sul pulsante **Fine** in qualunque momento, chiudere la procedura guidata e procedere alla configurazione manuale.

Questa sezione contiene i seguenti argomenti:

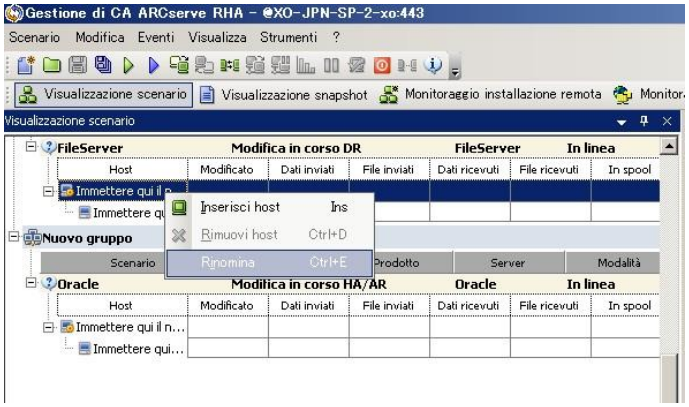
Definizione dei server master e di replica (a pagina 172)
Aggiunta di server di replica supplementari (a pagina 173)
Selezione di directory master e del relativo contenuto per la replica (a pagina 174)
Filtro dei file nelle directory master (a pagina 178)
Sincronizzazione chiavi di registro (a pagina 184)
Rilevamento automatico dei file di database per tutti i database (a pagina 189)
Selezione di directory principali di replica (a pagina 191)
Propagazione delle directory principali master a più host di replica (a pagina 193)
Operazioni dello scenario (a pagina 194)
Manutenzione degli host (a pagina 197)

Definizione dei server master e di replica

Ogni scenario viene automaticamente creato con un server master e uno di replica.

Per definire l'host master o di replica, procedere come segue.

1. Nel riquadro Scenario, fare clic con il pulsante destro del mouse sul testo **Immettere qui il nome dell'host master/replica** e selezionare **Rinomina** dal menu di scelta rapida. In alternativa, fare doppio clic sul testo desiderato.



   Immettere il nome host o l'indirizzo IP dell'host.

2. Premere il tasto **Invio** oppure fare clic in un punto qualsiasi fuori dal campo di testo.
3. Salvare le modifiche apportate facendo clic sul pulsante **Salva**.

   Dopo aver definito un nuovo host, sarà necessario definire le relative directory principali per la replica di dati.

   - Per definire le directory principali master, fare riferimento all'argomento Selezione di directory master e del relativo contenuto per la replica (a pagina 174).
   - Per definire le directory principali di replica, vedere Selezione di directory principali di replica (a pagina 191).

Aggiunta di server di replica supplementari

Durante la creazione guidata di uno scenario è possibile definire un solo server di replica per lo scenario. Per aggiungere ulteriori server di replica allo scenario, seguire le istruzioni fornite di seguito.

Per aggiungere server di replica supplementari, procedere come segue:

1. Dal riquadro Scenario, selezionare l'host (server master o di replica) al quale si desidera aggiungere un server. Fare clic su di esso con il pulsante destro del mouse e selezionare **Inserisci host** dal menu di scelta rapida oppure selezionare **Inserisci host** dal menu **Modifica**.

   Viene visualizzata una nuova voce di server di replica:

2. Definire il nuovo server di replica così come è stato definito l'altro host del server di replica e impostare le relative proprietà e directory principali.
3. Salvare le modifiche apportate facendo clic sul pulsante **Salva**.

Selezione di directory master e del relativo contenuto per la replica

In questa sezione viene descritta la modalità di selezione delle directory e dei file sul server master per la replica.

Note:

- L'utilizzo della finestra di dialogo **Directory principali master** è possibile solo se il modulo è installato e in esecuzione sull'host.
- Inoltre, è possibile selezionare chiavi di registro per la sincronizzazione, come descritto nella sezione Sincronizzazione chiavi di registro (a pagina 184).

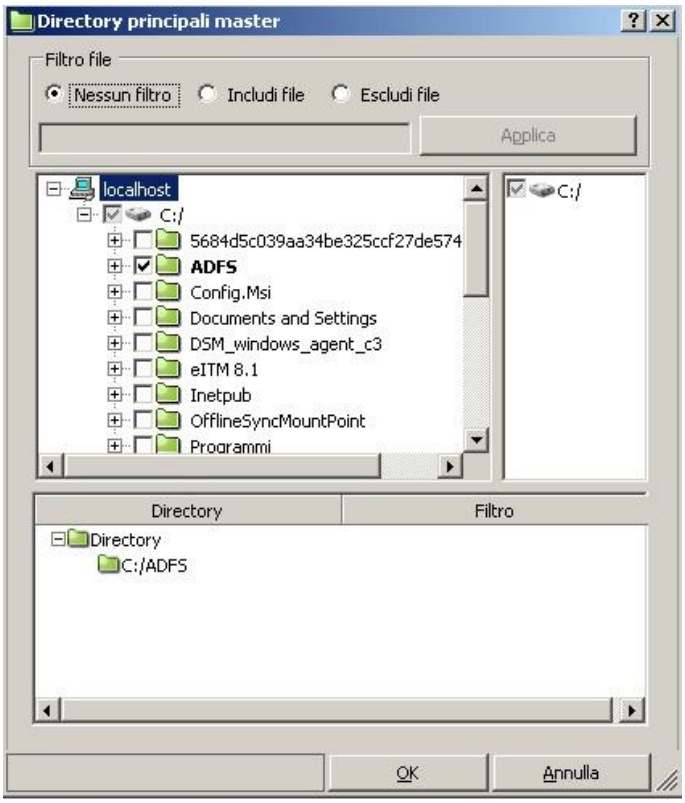
Importante: Si applicano speciali restrizioni ai percorsi UNC (\\server\share) delle directory principali remote. Il tipo di percorso non è supportato come origine (sul server master) per la replica in tempo reale. Tuttavia, può costituire la destinazione dei dati replicati in tempo reale, vale a dire essere utilizzato per memorizzare dati sul server di replica. In tal caso, le directory principali in questione possono persino supportare la replica ACL.

Per selezionare le directory del server master e il relativo contenuto, procedere come segue:

1. Nel riquadro Scenario, selezionare il nome del server master i cui dati si desidera replicare.
2. Nel riquadro Proprietà, fare clic sulla scheda **Directory principali** in basso. Vengono visualizzate le informazioni delle directory principali master.

3. Fare clic con il pulsante destro del mouse su qualsiasi punto del riquadro e selezionare **Sfoglia e seleziona le directory**. In alternativa, fare doppio clic sulla directory principale del server master denominata **Directory**.

   Viene visualizzata la finestra di dialogo **Directory principali master**:

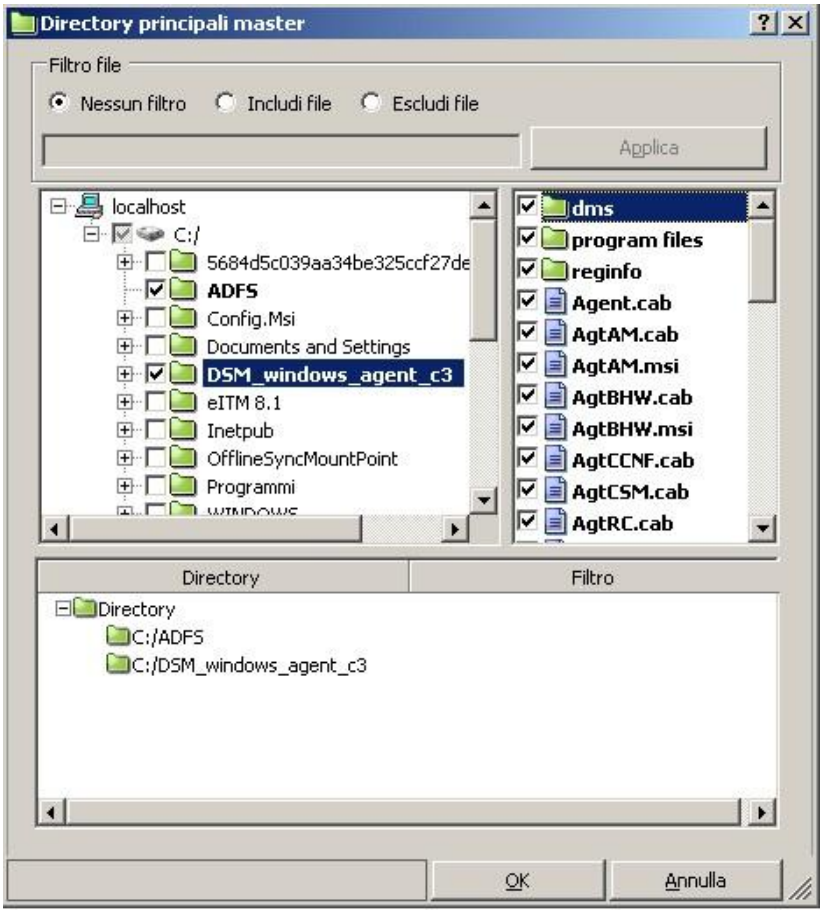


   La finestra di dialogo **Directory principali master** consta di due aree: l'area di sinistra mostra solo le directory e le sottodirectory, mentre l'area di destra mostra directory e sottodirectory, oltre ai file in esse contenuti. È possibile selezionare/deselezionare le caselle di controllo; se selezionate, le directory o i file relativi verranno replicati. Gli elementi le cui caselle non sono selezionate verranno ignorati.

4. Nell'area di sinistra della finestra di dialogo, selezionare le directory che parteciperanno allo scenario di replica del server master facendo clic sulle caselle di controllo pertinenti. Queste sono le Directory principali master. Dopo aver selezionato la casella di controllo, il nome della directory viene visualizzato in grassetto:

   Note:

   - Quando si selezionano le directory principali per i server master e di replica, la somma del numero di caratteri utilizzati per i nomi della directory principale e della sottodirectory non deve eccedere i 1024 caratteri.
   - Se una directory principale è una sottodirectory, resterà in grassetto e contrassegnata, inoltre la rispettiva directory padre apparirà contrassegnata con un segno di spunta di colore grigio.



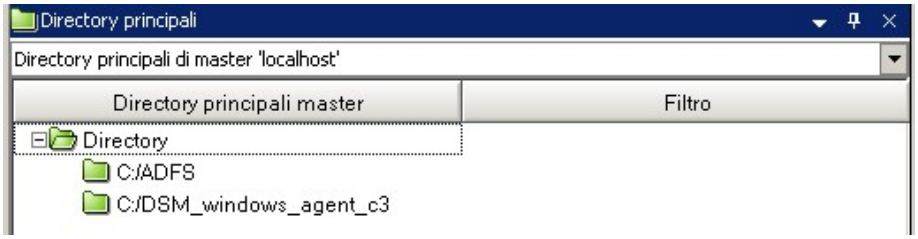
   Tutti i file e le sottodirectory appartenenti alla directory che viene evidenziata nell'area a sinistra verranno visualizzati nell'area a destra.

5. È possibile deselezionare le caselle di controllo delle sottodirectory e dei file specifici che compaiono nell'area a destra, in modo che vengano ignorati durante la replica.

   Nota: se si deselezionano le caselle di qualsiasi sottodirectory e file nell'area a destra, questi verranno ignorati, ma la directory principale verrà comunque selezionata. e contrassegnata da un segno di spunta di colore grigio.

6. Dopo aver selezionato tutte le directory e i file che desidera replicare, fare clic su **OK**.

   Le directory selezionate verranno visualizzate nel riquadro Directory principali sotto la colonna Directory principali master.



   Nota: quando si lavora con replica SQL Server, i database aggiunti alle directory principali selezionate dopo l'avvio della replica non verrà replicato.

Modifica dei nomi delle directory

È possibile modificare i nomi delle directory principali master. Tuttavia, quando si modifica il nome di una directory principale, è necessario verificare che tale directory esista realmente sul server master prima di eseguire lo scenario. Se si tenta di eseguire uno scenario con una directory principale del server master inesistente, lo scenario non verrà eseguito e verrà segnalato un errore critico.

Per modificare il nome di una directory

- Nella scheda Directory principali, selezionare la directory e immettere un nuovo nome utilizzando le convenzioni Windows;

  oppure

  Fare clic con il pulsante destro del mouse sul nome della directory e selezionare **Rinomina** dal menu di scelta rapida.

Rimozione delle Directory principali master

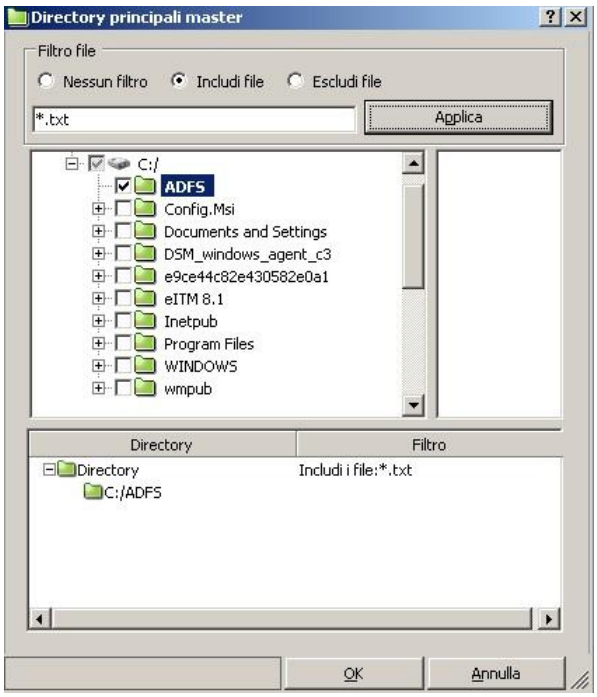
Per rimuovere una Directory principale master

- Fare clic con il pulsante destro del mouse sulla directory e scegliere **Rimuovi directory** dal menu di scelta rapida.

Filtro dei file nelle directory master

Le opzioni di filtro consentono di includere o escludere i file dalle directory principali master. Queste opzioni non consentono di selezionare/deselezionare le voci nella finestra di dialogo **Directory principali master**: è necessario farlo manualmente. Tuttavia, le opzioni di filtro consentono di ottimizzare la selezione delle directory e visualizzare solo i file che verranno replicati.

Ad esempio, se si sceglie di includere solo i file di testo sarà necessario selezionare le directory richieste e immettere i parametri di filtro. Quindi, solo i file di testo memorizzati in queste directory verranno visualizzati nell'area a sinistra della finestra di dialogo **Directory principali master**.



Le Directory principali master consentono di utilizzare una serie di caratteri di filtro, quali caratteri, stringhe, caratteri jolly, nomi di file o estensioni, ecc. Sono disponibili i seguenti caratteri jolly:

Nota: un "carattere" nel presente contesto si riferisce solo a caratteri alfanumerici.

- Un asterisco (*) consente di selezionare un numero qualsiasi di caratteri/cifre di tutti i tipi.
- Un punto interrogativo (?) consente di selezionare qualsiasi carattere o cifra numerica singoli.
- Un simbolo di cancelletto (#) consente di selezionare cancelletti o cifre.
- Una chiocciola (@) consente di selezionare chiocciole o caratteri alfabetici.
- L'immissione di altri caratteri (uno o più) consente di selezionare quei caratteri specifici.

La selezione di un determinato filtro si applica a tutti i file in tutte le directory selezionate nello scenario.

Le opzioni di filtro sono le seguenti:

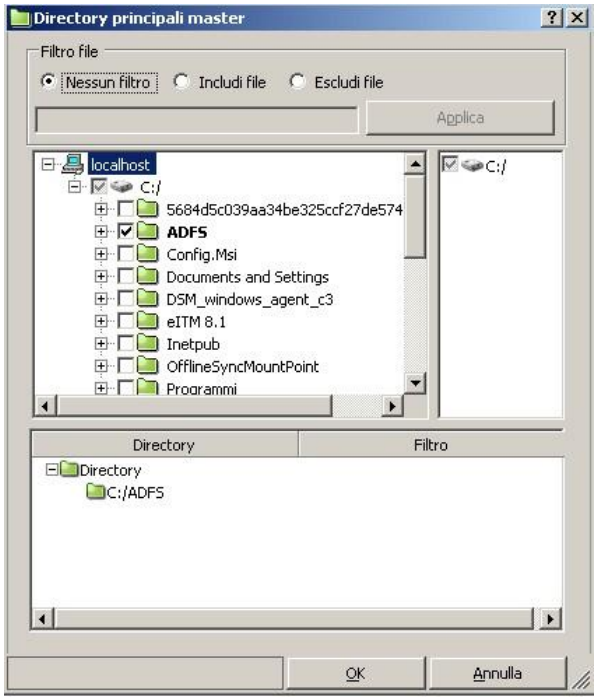
- **Nessun filtro**: verranno replicati tutte le directory e i file selezionati manualmente. Questa è l'opzione predefinita. Fare riferimento all'argomento Selezione di directory master e del relativo contenuto per la replica (a pagina 174).
- **Includi file**: SOLO i file o i tipi di file selezionati verranno replicati. Fare riferimento all'argomento Inclusione di file (a pagina 179).
- **Escludi file**: SOLO i file o i tipi di file selezionati verranno esclusi dalla replica, mentre tutti gli altri saranno inclusi. Fare riferimento all'argomento Esclusione di file (a pagina 182).

Includi file

Quando si utilizza **Includi file**, solo i file o i tipi di file immessi nella casella Filtro verranno inclusi nello scenario di replica e solo se appositamente selezionati. È necessario selezionare manualmente le directory in cui questi file sono memorizzati e, se si deseleziona manualmente un file in una casella di controllo, si ignora l'opzione **Includi file**.

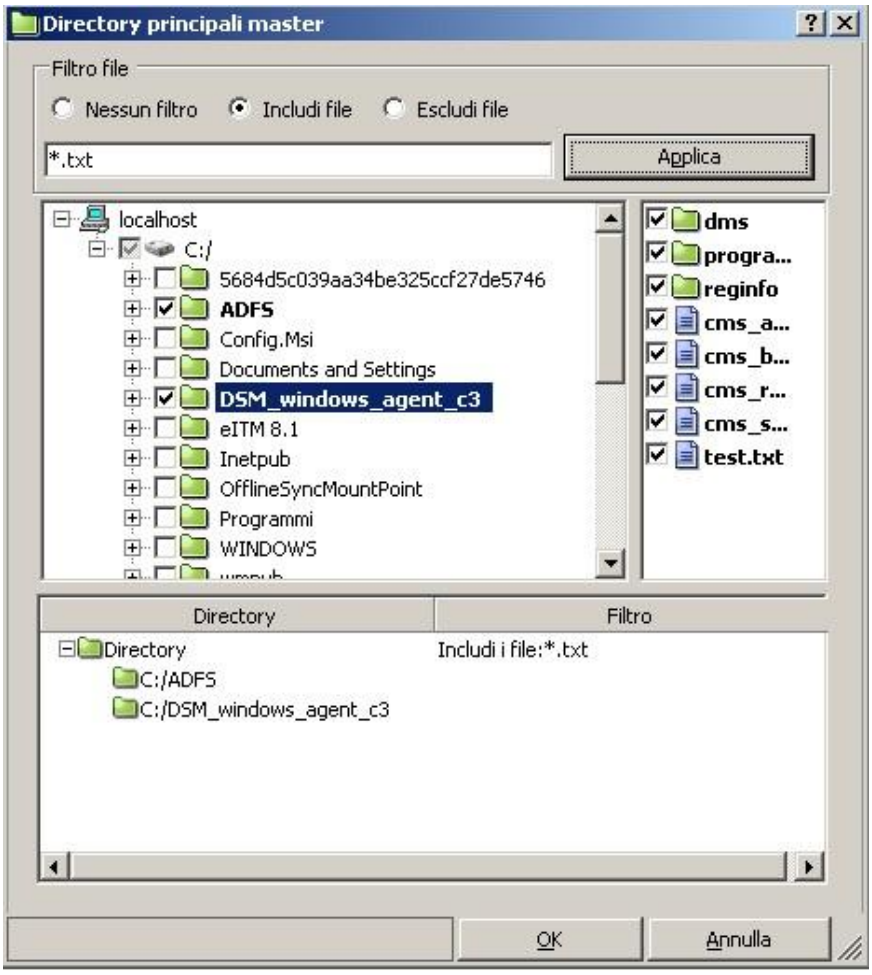
Per includere dei file, procedere come segue:

1. Nella finestra di dialogo **Directory principali master**, selezionare manualmente le directory a cui si desidera applicare il filtro.



Nota: in alternativa, è possibile selezionare manualmente la casella di controllo della directory DOPO aver immesso i parametri di filtro.

2. Fare clic sul pulsante di opzione **Includi file** nella parte superiore della finestra di dialogo **Directory principali master**. La casella Filtro viene abilitata con un carattere jolly di asterisco (*).



3. Immettere i tipi di file che si desidera includere nella casella Filtro utilizzando i caratteri di filtro appropriati. Ad esempio, includere tutti i file che terminano con estensioni *.txt *.exe. Separare le estensioni mediante uno spazio.

   Nota: NON utilizzare una virgola o un punto e virgola per separare le estensioni. Se un nome file include spazi vuoti, mettere tra virgolette ("") il nome completo del file.

4. Fare clic sul pulsante **Applica** per filtrare le directory selezionate in base ai parametri di filtro.

   Gli unici file che sono visualizzati nell'area a destra sono quelli che soddisfano i criteri di filtro.

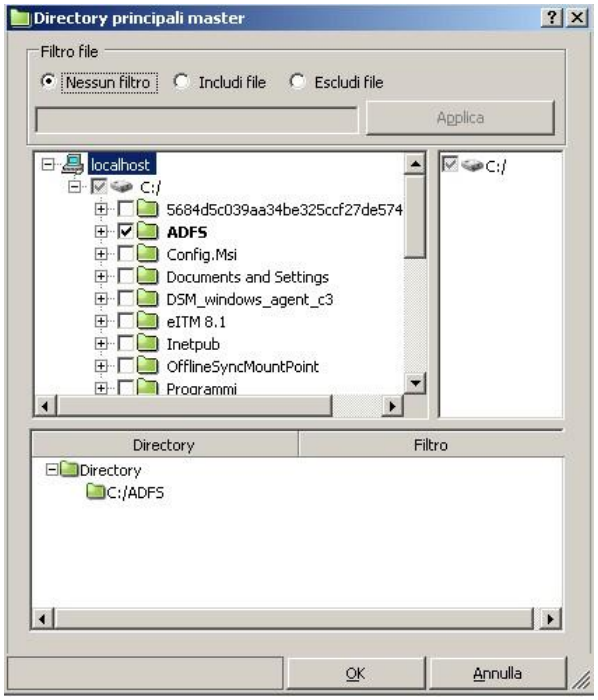
5. [Facoltativo] È possibile selezionare manualmente oppure cancellare individualmente directory e file. Questa operazione ignora l'opzione **Includi file** per quanto riguarda singole directory o file.
6. Fare clic su **OK** per salvare la directory principale selezionata e chiudere la finestra di dialogo **Directory principali master**.

Escludi file

Quando si utilizza **Escludi file**, lo scenario di replica ignora eventuali file filtrati (esclusi) e include tutti gli altri.

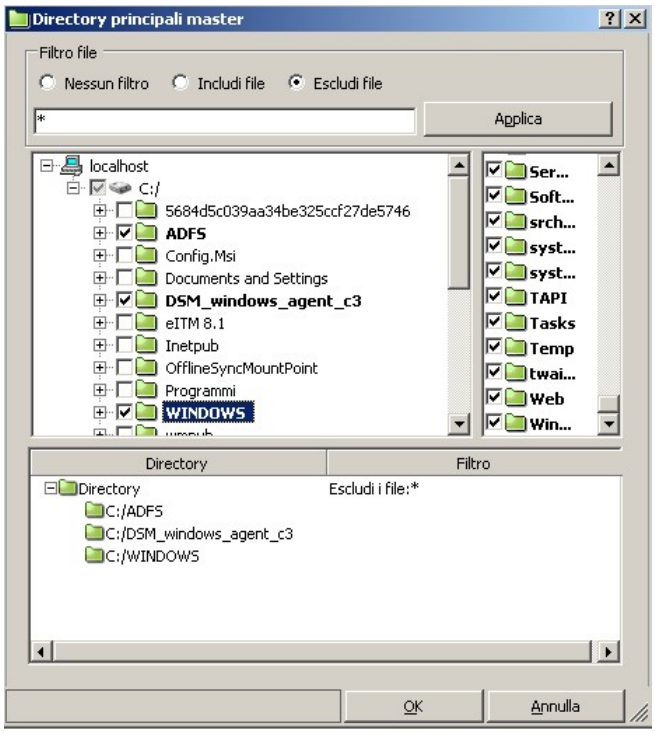
Per escludere dei file, procedere come segue:

1. Nella finestra di dialogo **Directory principali master**, selezionare manualmente le directory a cui si desidera applicare il filtro.



Nota: in alternativa, è possibile selezionare manualmente le directory DOPO aver immesso i parametri di filtro.

2. Fare clic sul pulsante di opzione **Escludi file** nella parte superiore della finestra di dialogo **Directory principali master**. La casella Filtro viene abilitata con un carattere jolly di asterisco (*).



   Immettere i tipi di file che si desidera escludere nella casella Filtro utilizzando i caratteri di filtro appropriati. Ad esempio, escludere tutti i file che terminano con estensioni *.bat *.dll. Separare le estensioni mediante uno spazio.

   Nota: NON utilizzare una virgola o un punto e virgola per separare le estensioni. Se un nome file include spazi vuoti, mettere tra virgolette ("") il nome completo del file.

3. Fare clic sul pulsante **Applica** per filtrare le directory selezionate in base ai parametri di filtro.

   I file esclusi non vengono visualizzati nell'area a destra e i file visualizzati saranno quelli che verranno replicati.

4. [Facoltativo] È possibile selezionare manualmente oppure cancellare individualmente directory e file. Questa operazione ignora l'opzione **Includi file** per quanto riguarda singole directory o file.

5. Fare clic su **OK** per salvare la directory principale selezionata e chiudere la finestra di dialogo **Directory principali master**.

Sincronizzazione chiavi di registro

Oltre alla sincronizzazione e alla replica dei dati applicazioni, Arcserve RHA consente di sincronizzare le chiavi di registro master e di replica. Mediante la funzione Sincronizzazione registro, è possibile selezionare le chiavi di registro sul server master da copiare sul server di replica e definire la frequenza di sincronizzazione. È possibile copiare le chiavi di registro master nella stessa posizione sul server di replica oppure modificare il nome e il percorso di archiviazione delle chiavi sincronizzate. Se nella struttura di replica sono presenti più host di replica, il processo di sincronizzazione del registro si applica a tutti gli host presenti. Le chiavi di registro non vengono replicate in tempo reale, bensì copiate dal server master al server di replica in base a una pianificazione a seconda della frequenza definita dall'utente.

Importante: Utilizzare questa funzione con cautela. La modifica delle chiavi di registro potrebbe comportare errori di sistema.

Note:

- Questa funzione non è valida per tutte le applicazioni che bloccano l'accesso alle rispettive chiavi di registro, né alle applicazioni con chiavi di registro non modificabili.
- Per impostazione predefinita, l'opzione Sincronizzazione registro è disabilitata.

Per la configurazione e l'esecuzione della funzione di sincronizzazione del registro è possibile utilizzare diversi passaggi.

1. Attivazione della proprietà Sincronizzazione registro. (a pagina 184)
2. Selezione delle chiavi di registro da sincronizzare sull'host master. (a pagina 186)
3. [Facoltativo] Selezione del nome e della posizione di archiviazione delle chiavi di registro sincronizzate sull'host di replica. (a pagina 187)
4. Avvio della sincronizzazione delle chiavi di registro mediante esecuzione dello scenario. (a pagina 127)

Attivazione dell'opzione Sincronizzazione registro

La prima fase della configurazione e dell'esecuzione dell'opzione Sincronizzazione registro è l'attivazione della stessa e la definizione della frequenza relativa.

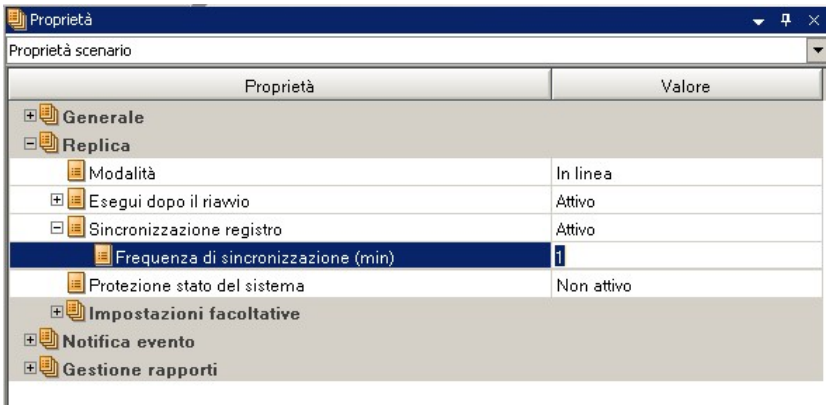
Nota: per configurare le proprietà Sincronizzazione registro, è necessario interrompere lo scenario. Per eseguire scenari che includono la sincronizzazione registro, è necessario eseguire Arcserve RHA utilizzando un account di amministratore di dominio.

Per attivare la proprietà Sincronizzazione registro, procedere come segue:

1. Nel riquadro Scenario, selezionare il nome dello scenario per cui si desidera attivare la proprietà **Sincronizzazione registro**.
2. Nel riquadro Proprietà, fare clic sulla scheda **Proprietà** in basso.

   L'elenco **Proprietà scenario** viene visualizzato nel riquadro.
3. aprire il gruppo **Replica**, selezionare la proprietà **Sincronizzazione registro** e impostarla su Attivo.

   La proprietà **Frequenza sincronizzazione** viene visualizzata nella proprietà **Sincronizzazione registro**.



4. Nella casella **Frequenza sincronizzazione**, immettere il numero di minuti che dovranno trascorrere fra ogni sincronizzazione delle chiavi di registro.
5. Salvare la configurazione impostata facendo clic sul pulsante **Salva** nella barra degli strumenti standard.

   È quindi necessario selezionare sull'host master le chiavi di registro da sincronizzare. (a pagina 186)

Selezione delle chiavi di registro per la sincronizzazione

Il secondo passaggio relativo alla configurazione e all'esecuzione dell'opzione Sincronizzazione registro consiste nel selezionare le chiavi di registro da sincronizzare sull'host master.

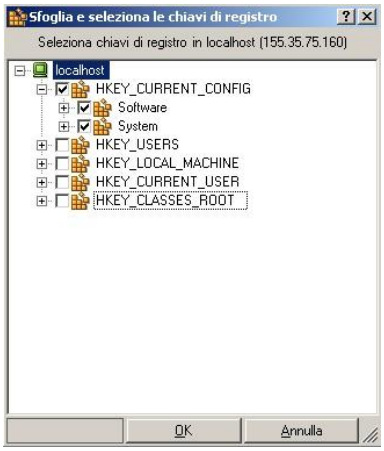
Note:

- Per selezionare le chiavi di registro per la sincronizzazione, è necessario interrompere lo scenario.
- Non è possibile selezionare chiavi di registro per la sincronizzazione dalla Creazione guidata scenario. Le chiavi di registro possono essere selezionate solo dal riquadro Proprietà della Gestione.
- Per la selezione vengono visualizzate unicamente le chiavi. Non è possibile selezionare valori specifici per la sincronizzazione.

Per selezionare le chiavi di registro per la sincronizzazione sul server master, procedere come segue:

1. Nel riquadro Scenario, selezionare il nome dell'host master di cui si desidera sincronizzare le chiavi di registro.
2. Nel riquadro Proprietà, fare clic sulla scheda **Directory principali** in basso. Le informazioni sulle **Directory principali master** vengono visualizzate nel riquadro.
3. Fare clic con il tasto destro del mouse sull'oggetto del registro di sistema corrispondente al sistema operativo in uso e selezionare **Sfoglia e seleziona le chiavi di registro** dal menu di scelta rapida. In alternativa, fare doppio clic sull'oggetto **Registro** corrispondente al sistema operativo in uso: **x86** o **x64**.

   Verrà visualizzata la finestra di dialogo **Sfoglia e seleziona le chiavi di registro**, contenente un elenco delle chiavi di registro dell'host master.



4. Fare clic sulle caselle di controllo delle chiavi di registro che si desidera sincronizzare.

   Note:

   - Non è possibile filtrare la selezione delle chiavi di registro.
   - Immettendo manualmente un nome e un percorso per una chiave di registro inesistente sul server master, potrebbe essere comunque possibile completare la verifica dello scenario, ma l'esecuzione di quest'ultimo verrà interrotta generando un messaggio di errore. Immettere unicamente i dati relativi a chiavi di registro esistenti per la replica.

5. Al termine della selezione di tutte le chiavi di registro da sincronizzare, fare clic su **OK**.

   Le chiavi di registro selezionate vengono visualizzate nel riquadro Directory principali nella colonna **Directory principali master**.

6. Salvare la configurazione impostata facendo clic sul pulsante **Salva** nella barra degli strumenti standard.

   Per impostazione predefinita, il sistema esegue automaticamente la configurazione delle chiavi di registro sul server di replica in modo da riflettere la configurazione delle chiavi di registro selezionate sul server master. Per modificare il nome e la posizione di archiviazione delle chiavi di registro sincronizzate sul server di replica, seguire le istruzioni riportate nella sezione seguente.

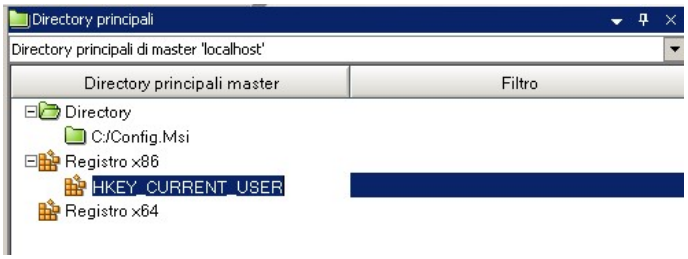
Selezione del nome e della posizione di archiviazione per le chiavi di registro sincronizzate

Il terzo passaggio previsto per la configurazione e l'esecuzione dell'opzione Sincronizzazione registro consiste nel selezionare il nome e la posizione di archiviazione delle chiavi di registro sincronizzate sull'host di replica. Per impostazione predefinita, il sistema configura le chiavi di registro del server di replica in modo che corrispondano alle chiavi di registro del server master selezionato, per cui questo passaggio è facoltativo.

Per selezionare il percorso di archiviazione delle chiavi di registro sincronizzate, procedere come segue:

1. Nel riquadro Scenario, selezionare il nome del server di replica in cui si desidera archiviare le chiavi di registro sincronizzate.

2. Nel riquadro Proprietà, fare clic sulla scheda **Directory principali** in basso. Le informazioni sulle directory principali di replica vengono visualizzate nel riquadro.



   Le chiavi di registro selezionate per la sincronizzazione sul server master vengono visualizzate sul server di replica nella stessa posizione e con lo stesso nome.

3. È possibile utilizzare due modalità per modificare il percorso e il nome predefiniti delle chiavi di registro sul server di replica in due modi.

   - Sostituire il percorso e il nome predefiniti con il percorso e il nome delle chiavi di registro esistenti:

     - Fare clic con il pulsante destro del mouse su un qualsiasi punto del riquadro e selezionare **Sfoglia e seleziona le chiavi di registro**. In alternativa, fare doppio clic sul nome della chiave di registro di replica specificata.

       Viene visualizzata la finestra di dialogo **Sfoglia e seleziona le chiavi di registro**.

     - Selezionare le caselle di controllo corrispondenti alle chiavi di registro da utilizzare e fare clic su **OK** per salvare la selezione.

   - Inserire manualmente il nuovo percorso e il nuovo nome per i valori predefiniti: fare doppio clic sul nome della chiave di registro nel riquadro Directory principali, quindi immettere manualmente un nuovo nome e un nuovo percorso.

4. Fare clic sul pulsante **Salva**sulla barra degli strumenti standard.

   Per avviare la sincronizzazione delle chiavi di registro, eseguire lo scenario (a pagina 127).

Rilevamento automatico dei file di database per tutti i database

Per facilitare la selezione delle directory per i database standard supportati da Arcserve RHA, le directory e i file di database vengono identificati nello scenario utilizzando API di database. Arcserve RHA visualizza la struttura del database ed effettua le selezioni appropriate. Tali selezioni possono essere modificate, se necessario.

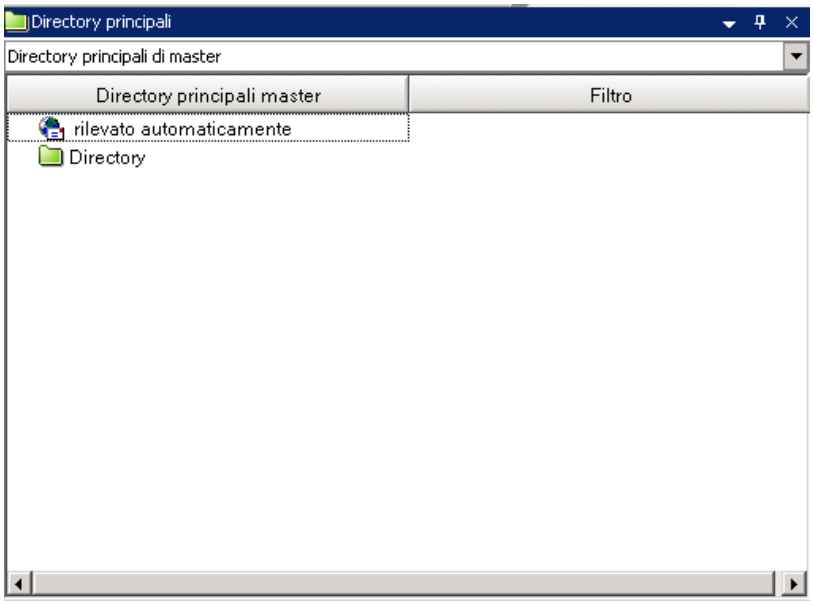
La funzione di rilevamento automatico di Arcserve RHA consente di rilevare automaticamente tutti gli oggetti di database, i file e le directory correlati sul server di database o di posta elettronica in uso, a livello locale o in rete. Questa funzione è attualmente disponibile per tutte le applicazioni supportate.

Nota: è possibile eseguire il rilevamento automatico solo se il modulo e il database Arcserve RHA sono installati e in esecuzione sul server master.

Per utilizzare il rilevamento automatico per la selezione di file di database:

1. Nel riquadro Scenario, selezionare lo scenario per il quale si desidera eseguire il rilevamento automatico del database ed assicurarsi che NON sia in esecuzione.
2. Nel riquadro Struttura, aprire la scheda **Directory principali** per il server master.

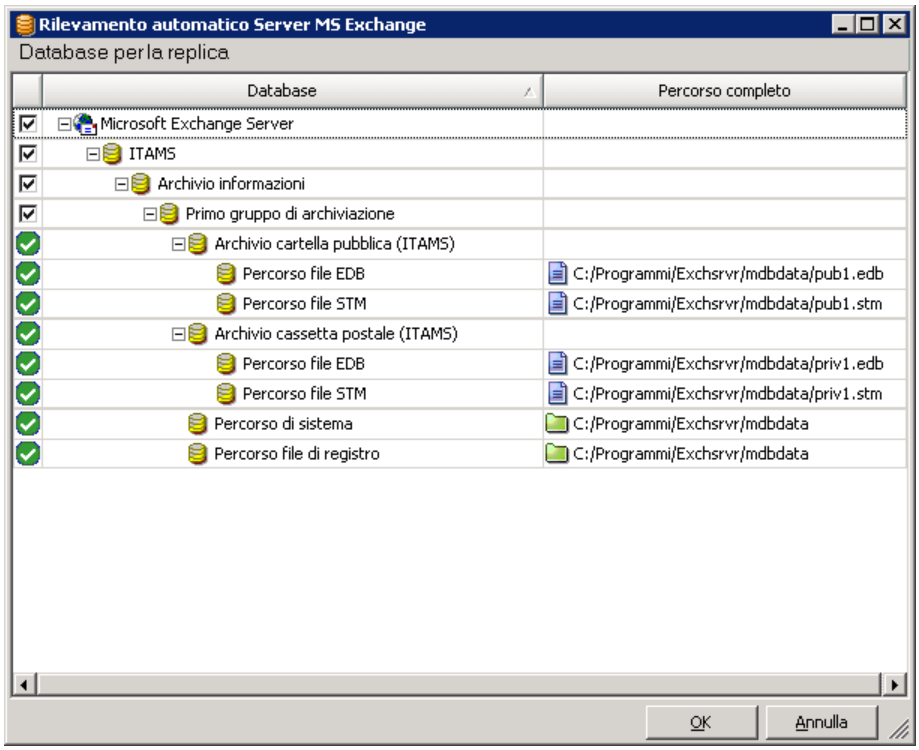
   L'icona **Rilevato automaticamente** relativa ai file di database viene visualizzata nella scheda Directory principali master.



3. Per avviare il rilevamento automatico, fare doppio clic sull'icona **Rilevato automaticamente**. In alternativa, selezionare l'opzione di **rilevamento automatico dei file di database** dal menu **Modifica**.

   Nota: se le credenziali utente utilizzate per accedere alla Gestione sono diverse da quelle richieste per l'utilizzo del modulo sul server di replica, viene visualizzata la finestra di dialogo **Credenziali utente**, in cui viene richiesto di immettere i dettagli dell'account di accesso per il server di replica selezionato.

   Viene visualizzata la finestra di dialogo di **rilevamento automatico**.



   La finestra di dialogo di **rilevamento automatico** visualizza tutte le directory e i file di database rilevati automaticamente.

4. Selezionare le caselle di controllo relative agli elementi che si desidera replicare e deselezionare quelle degli elementi da escludere dalla replica. Quindi, fare clic su **OK** per salvare la directory principale selezionata e chiudere la finestra di dialogo di **rilevamento automatico**.

Selezione di directory principali di replica

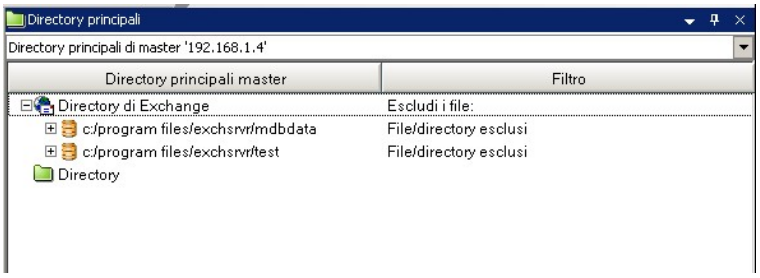
Affinché questa funzione sia disponibile è necessario selezionare le directory master. Per ciascuna Directory principale master, è necessario definire una Directory principale di replica su ciascun server di replica correlato.

Importante: Si applicano speciali restrizioni ai percorsi UNC (\\server\share) delle directory principali remote. Il tipo di percorso non è supportato come origine (sul server master) per la replica in tempo reale. Tuttavia, può costituire la destinazione dei dati replicati in tempo reale, vale a dire essere utilizzato per memorizzare dati sul server di replica. In tal caso, le directory principali in questione possono persino supportare la replica ACL.

Nota: è possibile sfogliare una directory solo se il modulo è installato e in esecuzione sul server selezionato.

Per selezionare le directory principali di replica, procedere come segue:

1. Nel riquadro Scenario, selezionare il nome del server di replica sul quale si desidera archiviare i dati replicati.
2. Nel riquadro Proprietà, fare clic sulla scheda **Directory principali** in basso. Le informazioni sulle directory principali di replica vengono visualizzate nel riquadro.

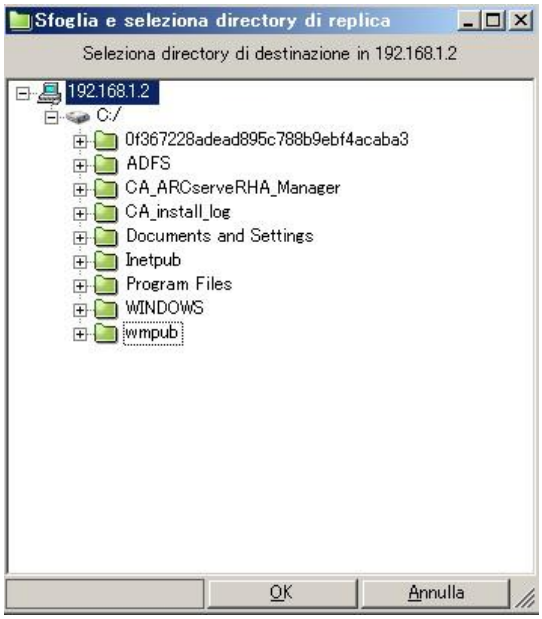


Importante: La creazione guidata dello scenario configura automaticamente le directory principali del server di replica in modo analogo alle directory principali del server master. Se si desidera mantenere questa configurazione, assicurarsi che la lettera dell'unità del server di replica sia la stessa di quella del server master e che le directory selezionate sul server di replica non contengano dati che si desidera salvare.

3. Per modificare le directory principali di replica predefinite, fare clic con il pulsante destro del mouse su qualsiasi punto del riquadro e selezionare **Sfoglia e seleziona le directory**. In alternativa, fare doppio clic sul nome della directory principale di replica specificata.

   Nota: se le credenziali utente utilizzate per accedere alla Gestione sono diverse da quelle richieste per l'utilizzo del modulo sul server di replica, viene visualizzata la finestra di dialogo **Credenziali utente**, in cui viene richiesto di immettere i dettagli dell'account di accesso per il server di replica selezionato.

   Arcserve RHA esegue la connessione al server di replica e visualizza la finestra di dialogo **Sfoglia e seleziona directory di replica**.

   Nella finestra **Sfoglia e seleziona directory di replica** è visualizzato l'elenco delle directory del server di replica.

4. Selezionare una directory di replica in cui memorizzare la corrispondente directory master. Ripetere la procedura per ciascuna directory master.

5. Affinché il processo di replica possa essere concluso con successo, verificare che l'utente che esegue il modulo disponga delle autorizzazioni per ciascuna directory principale di replica.

   Nota: la directory principale di replica non deve obbligatoriamente essere esistente. È possibile immettere il nome della directory selezionando la voce mediante le convenzioni standard di Windows e Arcserve RHA la creerà all'avvio della replica.

6. Fare clic su **OK** per salvare la directory selezionata e chiudere la finestra di dialogo **Sfoglia e seleziona directory di replica**.

Propagazione delle directory principali master a più host di replica

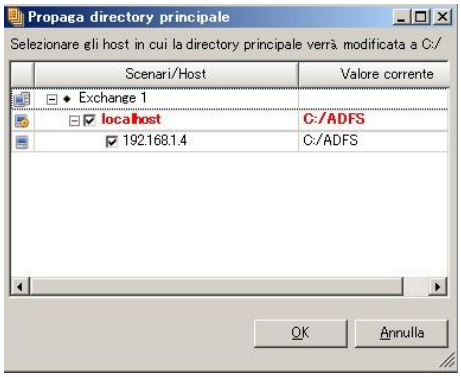
Arcserve RHA consente di propagare le directory principali impostate per l'host master a più host di replica contemporaneamente. Anziché configurare separatamente le directory principali di ciascun host di replica, con un solo clic è possibile distribuire la directory principale di un host master al numero di host di replica desiderato. Questa opzione è particolarmente utile per uno scenario che include più host di replica.

Nota: per applicare direttamente le modifiche alle directory principali, lo scenario deve essere arrestato.

Per propagare le directory principali, procedere come segue:

1. Nel riquadro Scenario, selezionare l'host master di cui si desidera propagare le directory.
2. Nel riquadro Struttura, fare clic sulla scheda **Directory principali** in basso. Le informazioni sulle Directory principali master vengono visualizzate nel riquadro.
3. Nel riquadro Directory principali master, fare clic con il tasto destro del mouse sulla directory principale che si desidera propagare e selezionare **Propaga il valore** dal menu di scelta rapida.

4. Fare clic sul comando **Propaga il valore**. Viene visualizzata la finestra di dialogo **Propaga il valore**.



   Nella finestra di dialogo vengono visualizzati gli host master e di replica inclusi nello scenario. La directory principale selezionata per la propagazione viene visualizzata sopra la tabella **Scenari/Host** e nella colonna **Valore corrente** contrassegnata in rosso.

5. Per propagare la directory principale agli host di replica, fare clic su **OK**.

   Nota: per escludere gli host dalla propagazione del valore, deselezionare le relative caselle di controllo e fare clic su **OK**.

6. Una volta chiusa la finestra di dialogo **Propaga valore**, fare clic sul pulsante **Salva tutto** sulla barra degli strumenti standard per salvare e applicare le modifiche a tutti gli scenari.

Operazioni dello scenario

Le sezioni seguenti descrivono le operazioni dello scenario:

- Salvataggio degli scenari (a pagina 195)
- Rimozione di scenari (a pagina 195)
- Esportazione di scenari (a pagina 196)
- Importazione di scenari (a pagina 197)

Salvataggio degli scenari

Esistono due metodi per salvare gli scenari: il salvataggio di singoli scenari oppure il salvataggio globale di tutti gli scenari.

Per salvare gli scenari

- Nel riquadro Scenario, selezionare lo scenario e fare clic sull'icona **Salva** oppure selezionare l'opzione **Salva** dal menu **Scenario**.

  oppure

- Fare clic sull'icona **Salva tutto** oppure selezionare **Salva tutto** dal menu **Scenario**, per salvare tutti gli scenari nella Gestione.

Rimozione di scenari

Importante: Prima di rimuovere uno scenario, assicurarsi di averlo eliminato in modo permanente. Non è possibile annullare l'azione.

Per rimuovere uno scenario, procedere come segue:

1. Dal riquadro Scenario, selezionare lo scenario e fare clic su di esso con il pulsante destro del mouse.

   Verrà visualizzato un menu di scelta rapida.

2. Scegliere **Rimuovi** dal menu di scelta rapida.

   Viene visualizzato un messaggio in cui viene richiesto di confermare la rimozione.

3. Fare clic su **OK**. Lo scenario viene rimosso in modo permanente.

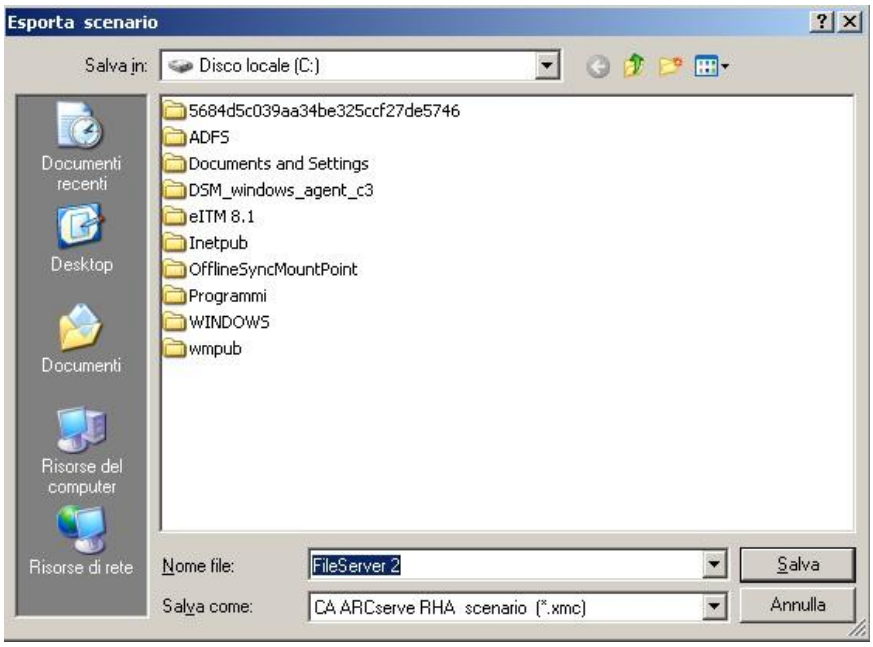
Esportazione di scenari

È possibile esportare scenari in altre posizioni allo scopo di riutilizzarli.

Per esportare uno scenario, procedere come segue:

1. Dal riquadro Scenario, selezionare lo scenario che si desidera esportare. Quindi, fare clic con il pulsante destro del mouse su**Esporta**, oppure selezionare l'opzione **Esporta** dal menu **Scenario**.

   Viene visualizzata la finestra di dialogo **Esporta scenario**.



2. Dare un nome allo scenario e fare clic sul pulsante **Salva** per salvarlo.

   Lo scenario viene salvato come file *.xmc.

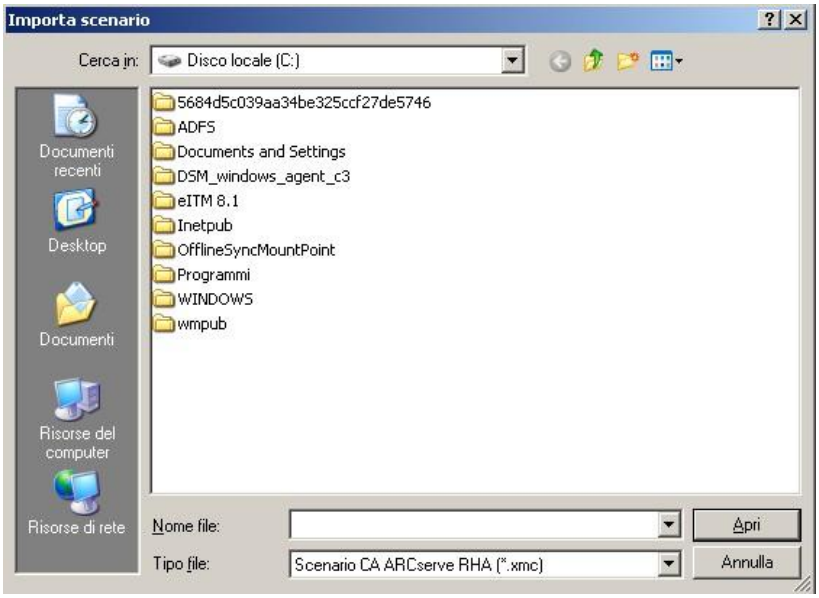
Importazione di scenari

È possibile importare file .xmc che contengono scenari salvati sulla Gestione. Utilizzare questa opzione se si desidera spostare gli scenari da una workstation all'altra, oppure se si desidera utilizzare scenari precedenti conservati nel sistema.

Per importare uno scenario, procedere come segue:

1. Dal riquadro **Scenario**, fare clic su **Gruppo scenari**.
2. Dal menu **Scenario**, scegliere l'opzione **Importa**.

   Viene visualizzata la finestra di dialogo **Importa scenario**.



3. Individuare lo scenario da importare e fare clic su **Apri**.

   Lo scenario verrà importato nella Gestione e verrà visualizzato nel riquadro Scenario.

4. Selezionare le opzioni necessarie e fare clic su **OK**.

Manutenzione degli host

Le sezioni seguenti illustrano l'opzione di manutenzione host e le modalità di preparazione degli host per procedure di manutenzione.

Informazioni sull'opzione di manutenzione host

L'opzione Manutenzione host consente di eseguire procedure di manutenzione, come il riavvio di un host oppure lo spostamento di gruppi tra nodi cluster Microsoft, senza dover eseguire la risincronizzazione al termine del processi. Di norma, quando il processo di replica in linea viene interrotto in maniera critica, è necessario confrontare i dati tra gli host di origine e destinazione per renderli identici, allo scopo di garantire l'integrità dei dati prima che sia possibile procedere con la replica. Il processo di risincronizzazione consuma tempo e risorse. L'opzione Manutenzione host consente di preparare il sistema replicato per le procedure di manutenzione pianificata ed evitare la risincronizzazione.

Gli host che è possibile preparare per la manutenzione devono partecipare agli scenari in esecuzione. La preparazione viene eseguita su un solo host per volta, ma tale host può partecipare a più scenari. In questi scenari, l'host può fungere sia da server master sia da server di replica. Quando un host partecipa a uno scenario che non è in esecuzione, i preparativi correlati a questo scenario non avranno luogo. Ad esempio, un host può partecipare agli scenari file server ed Exchange. Se, prima di iniziare a preparare l'host, lo scenario file server non è in esecuzione, solo i servizi di Exchange verranno interrotti durante la preparazione, e le condivisioni del server resteranno intatte.

Quando l'host selezionato funge da server master, durante il processo di preparazione verranno interrotti i servizi DB o le condivisioni file, a seconda del tipo di scenario. Quindi, tutte le modifiche apportate fino a quel momento verranno passate al server di replica. Quando il server di replica avrà inviato al server master la conferma dell'applicazione di tutte le modifiche e della verifica dell'integrità dei dati, lo scenario verrà sospeso e l'host è pronto per la manutenzione. Quando l'host selezionato funge da server di replica, le modifiche ad esso inviate verranno applicate e il server master smette di inviare nuove modifiche. Nel frattempo, le nuove modifiche verranno salvate nello spool del server master per il futuro aggiornamento. Quindi, lo scenario viene sospeso e l'host viene dichiarato pronto per la manutenzione.

Al completamento delle procedure di manutenzione, Arcserve RHA riprenderà in modo regolare la replica in tempo reale, evitando eventuali ritardi o interruzioni causati dalla risincronizzazione.

Importante. Questa opzione è valida solo per le applicazioni di database e file server e supporta scenari Replication e HA. Tuttavia, quando si utilizza questa opzione per gli scenari di file server e vi sono applicazioni in esecuzione a livello locale sull'host che si desidera riavviare, sarà necessario arrestarle manualmente prima di avviare la preparazione della manutenzione dell'host, quindi riavviarle manualmente al termine della manutenzione.

Preparazione degli host per le procedure di manutenzione

Per preparare gli host per le procedure di manutenzione, procedere come segue:

1. Nel riquadro Scenario, verificare che gli scenari i quali host si desidera riavviare siano in esecuzione.

   Note:

   - Non è necessario eseguire tutti gli scenari ai quali partecipa l'host. La preparazione verrà eseguita solo sulle parti che implicano lo scenario in esecuzione; ad esempio, i servizi di Exchange nel caso di uno scenario Exchange.
   - La preparazione della manutenzione dell'host non può essere eseguita durante la sincronizzazione. Se uno scenario è in corso di sincronizzazione, attenderne il completamento.

2. Fare clic sul pulsante **Avvia manutenzione host** oppure selezionare **Avvia manutenzione host** dal menu **Strumenti**.

   Viene visualizzata la procedura guidata **Manutenzione host**.

   La procedura guidata **Manutenzione host** consente di visualizzare tutti gli host che partecipano agli scenari in esecuzione.

   Nota: se lo stesso host compare sotto nomi/IP differenti in diversi scenari, verrà visualizzato più volte in questa schermata.

3. Selezionare l'host che si desidera preparare per la manutenzione e fare clic su **Avanti**.

   Viene visualizzata la pagina **Procedura di manutenzione**.

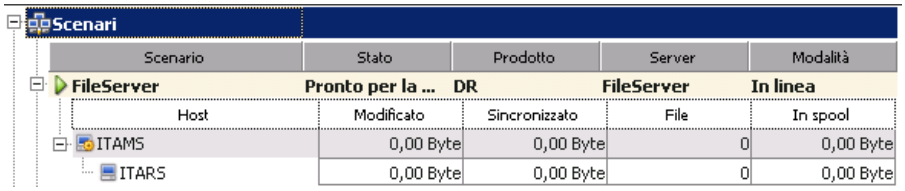
   Nella schermata **Procedura di manutenzione** sono visualizzate le informazioni dettagliate relative agli scenari ai quali partecipa l'host selezionato.

4. Nella sezione **Selezionare la procedura di manutenzione** a sinistra, selezionare l'operazione che si desidera eseguire e fare clic sul pulsante **Avvia**.

   Nel riquadro Eventi, verrà visualizzato il messaggio **Preparazione per il riavvio in corso**. Quindi, verrà visualizzato un altro messaggio: **Pronto per il riavvio**.

   Nota: se viene visualizzato il messaggio **Non pronto per il riavvio**, ciò significa che la preparazione non è andata a buon fine; dopo aver riavviato l'host, verrà eseguita la risincronizzazione.

   Allo stesso tempo, nel riquadro Scenario, lo stato dello scenario viene modificato in **Pronto per la manutenzione host**.



Nota: lo stato dello scenario che compare nel riquadro Scenario si riferisce solo allo stato dell'host master. Di conseguenza, se l'host che si sta preparando per la manutenzione funge da server di replica, non sarà possibile visualizzarne lo stato modificato nel riquadro Scenario, ma solo sul riquadro Eventi e nel monitor di manutenzione host.

5. Per visualizzare lo stato dell'host selezionato e degli scenari a cui esso partecipa, dal menu **Visualizza** scegliere l'opzione **Visualizzazione attiva**, **Monitoraggio manutenzione host** oppure fare clic sul pulsante **Monitoraggio manutenzione host** .

   Viene visualizzata la vista **Monitoraggio manutenzione host**.

   Nella vista Monitoraggio manutenzione host sono visualizzate tutte le richieste di preparazione per la manutenzione. Una richiesta di manutenzione scompare dal Monitor quando lo scenario interessato viene interrotto o eseguito. Non è possibile eseguire azioni nel Monitor, che serve solo a visualizzare informazioni sullo stato delle richieste correnti. L'unica operazione disponibile è l'apertura della procedura guidata di manutenzione degli host facendo clic in qualsiasi punto della schermata e selezionando **Avvia manutenzione host**.

   In questo Monitor, il nome host visualizzato è il suo nome completo e non il nome con il quale compare negli scenari. Tutti gli scenari ai quali partecipa questo host verranno visualizzati nel Monitor.

6. Dopo aver ricevuto il messaggio che informa che l'host è pronto per il riavvio, sarà possibile riavviare l'host oppure scambiare i gruppi tra i nodi cluster. Dopo aver completato le procedure di manutenzione, il processo di replica riprenderà automaticamente, senza eseguire la risincronizzazione.

Nota: se dopo aver preparato l'host per la manutenzione si è deciso di non riavviarlo e di mantenere in esecuzione i relativi scenari, sarà necessario interrompere gli scenari ed eseguirli nuovamente.

Capitolo 8: Impostazione delle proprietà

In questo capitolo vengono descritte le modalità di configurazione delle proprietà dello scenario e viene fornito l'elenco delle proprietà dello scenario, i valori corrispondenti e una spiegazione per ciascuna proprietà.

Questa sezione contiene i seguenti argomenti:

Configurazione delle proprietà di uno scenario (a pagina 201)
Nozioni fondamentali sulle proprietà dello scenario (a pagina 202)
Pianificazione della sincronizzazione (a pagina 211)
Impostazione delle proprietà del server master e di replica (a pagina 215)
Modifica della configurazione durante l'esecuzione di uno scenario (a pagina 240)
Protezione dello stato del sistema (a pagina 241)

Configurazione delle proprietà di uno scenario

Le proprietà dello scenario determinano il comportamento predefinito dell'intero scenario in merito al metodo di sincronizzazione, alle modalità di replica, alla notifica eventi, alla generazione di rapporti e molto altro.

Note:

- Il riquadro Proprietà e le relative schede (Directory principali, Proprietà, Statistiche) sono sensibili al contesto e vengono modificate ogni volta che si seleziona un diverso nodo da una cartella di scenari.
- È possibile che alcune proprietà dello scenario vengano modificate mentre lo scenario è in esecuzione. Per ulteriori informazioni, si rimanda alla sezione Modifica della configurazione dello scenario. (a pagina 240) Per modificare altre proprietà dello scenario, è necessario interrompere lo scenario stesso.

Ciascuno scenario viene identificato da uno specifico tipo di prodotto, tipo di server e ID di scenario univoco. Non è possibile modificare i valori di questi elementi.

Per impostare o modificare le proprietà di uno scenario:

1. Dal riquadro Scenario, selezionare lo scenario del quale si desidera configurare le proprietà. Nel riquadro Struttura a sinistra viene visualizzato l'elenco Proprietà scenario.

   Nota: uno scenario in esecuzione ha lo sfondo di colore grigio, mentre gli scenari non in esecuzione hanno uno sfondo di colore bianco.

2. Se lo scenario è in esecuzione e la proprietà che si desidera modificare non è modificabile durante l'esecuzione dello scenario, fare clic sul pulsante **Interrompi** della barra degli strumenti. Lo scenario viene interrotto.

3. Nell'elenco Proprietà scenario, aprire il gruppo desiderato, selezionare la proprietà richiesta e selezionare o immettere i valori appropriati. È possibile immettere manualmente alcuni valori nel campo di una casella di modifica mentre è possibile selezionarne altri da una casella combinata o un controllo IP facendo clic sul valore predefinito.

4. Dopo aver impostato le proprietà richieste, fare clic sul pulsante **Salva** nella barra degli strumenti standard per salvare e applicare le proprie modifiche. Riavviare lo scenario.

Nozioni fondamentali sulle proprietà dello scenario

In questa sezione vengono elencate le proprietà dello scenario, i valori corrispondenti, e viene fornita una spiegazione per ciascuna proprietà. Le proprietà vengono classificate in base alla loro posizione nel relativo gruppo di proprietà:

- Generale (a pagina 202)
- Replica (a pagina 203)
- Notifica di eventi (a pagina 208)
- Gestione rapporti (a pagina 210)
- Configurazione delle proprietà di uno scenario (a pagina 201)

Proprietà generali

Le proprietà in questo gruppo non possono essere modificate. Le proprietà Tipo prodotto e Tipo server vengono impostate durante la creazione di un nuovo scenario. La proprietà ID scenario viene assegnata automaticamente dal sistema. Per modificare tali proprietà è necessario creare un nuovo scenario.

Tipo prodotto

Replication o High Availability (HA).

Tipo server

Il tipo di server di applicazioni o database che partecipa allo scenario.

ID Scenario

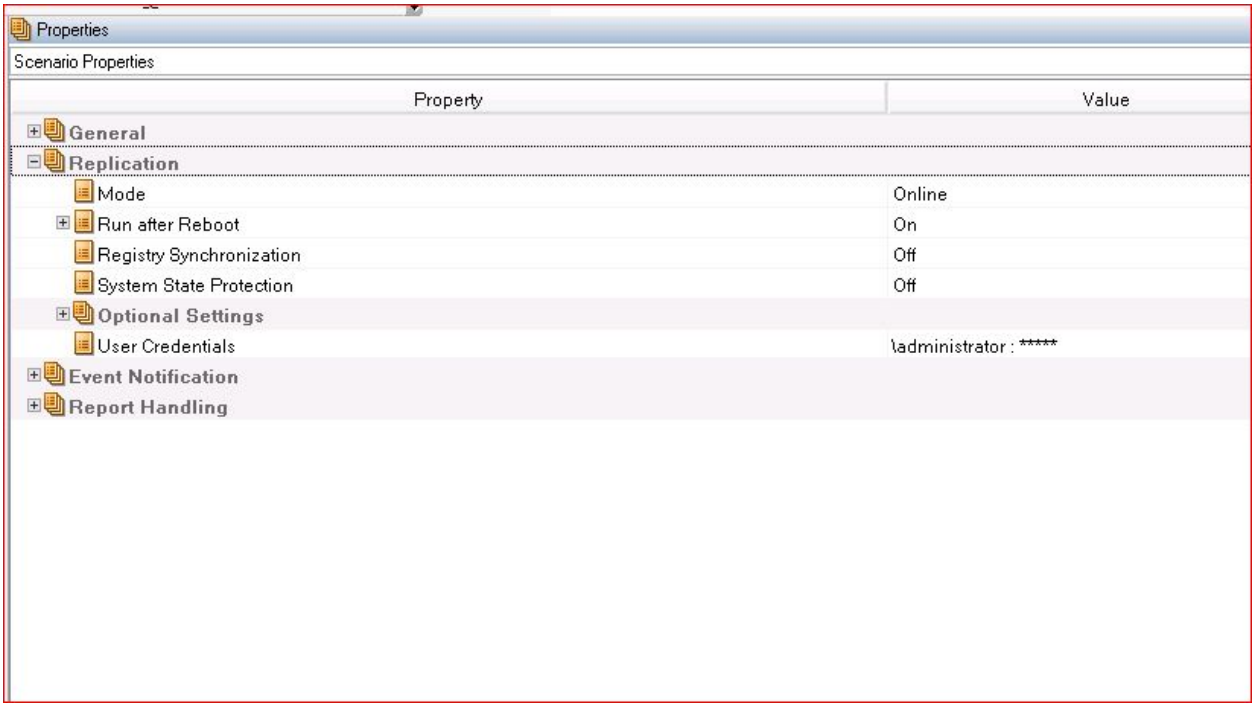
L'ID univoco dello scenario.

Proprietà di replica

La replica include le seguenti proprietà:

- Modalità

  Arcserve RHA supporta le seguenti modalità di replica:



- In linea

  La modalità di replica in linea attiva la replica in tempo reale. Le modifiche verranno replicate continuamente, in tempo reale, mediante il driver XOMF.

  La modalità in linea replica tutte le modifiche apportate ai file, anche quelli che sono sempre aperti (come nel caso della maggior parte dei database e dei server di posta elettronica). Questa modalità mantiene l'ordine delle operazioni del file system. In questa modalità, il modulo registra tutte le operazioni di I/O correlate alle directory principali nei file diario. I file diario vengono poi inviati ai server di replica, dove le operazioni che erano state registrate nel diario vengono riprodotte sui file replicati.

- Pianificato

  La modalità di replica pianificata è semplicemente una sincronizzazione eseguita in maniera automatica. È possibile avviare la sincronizzazione sia mediante attivazione manuale o in base a un piano predefinito, ad esempio a intervalli di poche ore o una volta al giorno. Questa modalità di replica non differisce in principio da una sincronizzazione eseguita come parte della replica di inizializzazione. Benché in questa modalità non venga eseguita la replica in linea, le modifiche in linea apportate durante la sincronizzazione verranno replicate.

  Quando l'opzione **Pianificazione** è selezionata, sono abilitate due opzioni:

  - **Per richiesta utente**

    La sincronizzazione viene attivata da un utente che la esegue dalla Gestione oppure da PowerShell.

  - **Attività settimanali**

    Nell'impostazione Attività settimanali della modalità Pianificata, i server vengono sincronizzati a intervalli fissi pianificati. Quando si seleziona questa opzione, è necessario impostare la pianificazione per la sincronizzazione ricorrente.

    Per una descrizione dettagliata della pianificazione della sincronizzazione, consultare la sezione Pianificazione della sincronizzazione (a pagina 211).

- Replica periodica

  Le modifiche apportate ai file non vengono replicate continuamente, bensì periodicamente aggregate. Le modifiche aggregate vengono propagate alla replica in base a una pianificazione. In Proprietà scenario, sotto Replica, espandere Modalità e impostare le proprietà di pianificazione e le impostazioni di pianificazione.

  Quando vengono applicati i dati di replica, potrebbero verificarsi ritardi, a seconda delle dimensioni dei dati e del numero di file da applicare, in quanto il processo garantisce la coerenza dei dati. È possibile impostare il parametro KeepUndoForPeriodic su false per arrestare la generazione dei file di ripristino ed accelerare l'applicazione delle modifiche aggregate. Ad ogni modo, tale impostazione non è consigliabile per scenari di database. Il parametro menzionato si trova nel file ws_rep.cfg.

- Esecuzione dopo il riavvio

  Se il server master viene riavviato, Arcserve RHA risincronizza automaticamente il server master e il server di replica dopo il riavvio.

  - Sincronizzazione automatica

    La sincronizzazione garantisce che un gruppo di cartelle e di file su un server di replica che partecipa a uno scenario sia identico al set presente sul server master.

- Tipo di sincronizzazione
  - **Sincronizzazione file**

    Consente di confrontare i file sui server master e di replica e, quando sono diversi, copia gli interi file mancanti o modificati dal server al server di replica.

    Per sincronizzare i dati per la prima volta, è necessario scegliere la modalità di Sincronizzazione file per ogni scenario. Nei casi successivi, questo tipo di sincronizzazione è più adeguato al file server (un elevato numero di file di dimensioni medie e piccole), preferibilmente selezionando l'opzione **Ignora file della stessa dimensione/data**. In tal modo, si potrebbe ridurre in maniera significativa il tempo di sincronizzazione.

  - **Sincronizzazione a blocchi**

    Esegue un confronto blocco per blocco dei file sui server master e di replica, quindi copia solo i blocchi che sono differenti. Quando vi sono differenze tra un file e l'altro, piuttosto che richiedere il trasferimento dell'intero file, la sincronizzazione a blocchi trasferisce solo le modifiche.

    La sincronizzazione a blocchi è il metodo appropriato per le applicazioni di database, quali MS Exchange, Oracle o SQL Server. Per utilizzare questo metodo, deselezionare l'opzione **Ignora file della stessa dimensione/data** (a meno che i file di database siano chiusi sul server master).

- Ignora file con la stessa dimensione/data

  Consente di non eseguire il confronto di file con lo stesso percorso, nome, dimensione e data di modifica, supponendo che tali file siano identici.

  Selezionare questa opzione quando si è assolutamente certi che i file di questo tipo siano identici. Questa opzione è più idonea agli scenari file server, ma non è appropriata per i file di database per applicazioni quali Exchange, SQL o Oracle, dal momento che questi database modificano i file (lasciandoli aperti) senza cambiare l'ora di modifica del file. Utilizzare questa opzione negli scenari di database solo quando i database sincronizzati vengono smontati e i file sono chiusi sul server master.

  Questa opzione può ridurre radicalmente il tempo di sincronizzazione complessivo, ma occorre ricordare che ciò avviene alle spese della verifica del contenuto.

- Sincronizzazione registro

  Se impostata su Attivo, questa opzione consente di sincronizzare le chiavi di registro master e di replica su base pianificata.

  Per una descrizione dettagliata della sincronizzazione del registro, fare riferimento all'argomento Sincronizzazione chiavi di registro (a pagina 184).

- Protezione stato del sistema

  Se impostata su Attivo, questa opzione consente di salvare le snapshot del sistema e di avviare i file del server master sul server di replica. Per attivare l'opzione, è necessario impostare la Pianificazione protezione stato del sistema e definire l'host di replica su cui archiviare le snapshot. Per una descrizione dettagliata, fare riferimento all'argomento Protezione dello stato del sistema (a pagina 241).

- Impostazioni facoltative

  - Replica attributo compresso NTFS

    (Solo per Windows) Replica l'attributo compresso dei file o delle directory durante la sincronizzazione e la replica.

  - Replica elenchi di controllo

    Questa impostazione consente di replicare gli elenchi di controllo di accesso (ACL) per file e directory durante la sincronizzazione e la replica.

    Memorizza nomi dell'account locale **(solo per Windows)**

    Il modulo RHA memorizza il nome locale nel computer di replica. Prima di eseguire lo scenario, è necessario creare manualmente gli stessi utenti o gruppi locali sul computer master e di replica. Utilizzare questa proprietà per ambienti di gruppo di lavoro.

  - Sincronizzazione di condivisioni Windows

    Se è stata impostata una directory per consentire la condivisione, l'attivazione di questa opzione consente di duplicare la proprietà nella directory replicata. Ciò si verifica solo durante la sincronizzazione e sul sistema operativo Windows.

  - Mantieni l'attributo di archivio sulla replica

    Se il master e la replica sono identici, non modificare l'attributo di archiviazione sulla replica durante la sincronizzazione.

  - Impedisci la risincronizzazione automatica in seguito a un errore

    Un errore grave non comune sul server master può interrompere la continuità della replica. In questo caso, l'attivazione di questa opzione impedisce che venga eseguita la risincronizzazione automatica. Quando questa opzione è disattivata, la risincronizzazione viene avviata automaticamente al verificarsi di un errore.

- Interrompi lo scenario quando un disco/spool è pieno

  Per scenari configurati con server di replica multipli, questa proprietà consente di interrompere solo la replica interessata o l'intero scenario quando uno spool o il disco di una replica sono pieni. Impostare questa proprietà su Non attivo per interrompere solo la replica interessata e su Attivo per interrompere l'intero scenario.

- Numero di stream

  Questa proprietà consente di utilizzare più efficacemente la larghezza di banda in un ambiente con latenza elevata (WAN). È possibile utilizzare l'interfaccia utente o il file ws_rep.cfg per impostare questa proprietà su un valore tra 1 e 10. Il valore predefinito utilizza un solo stream. Qualunque valore impostato nel file ws_rep.cfg ha la prevalenza sul valore predefinito. Al contrario, qualsiasi valore impostato nell'interfaccia utente prevale sul valore impostato nel file ws_rep.cfg.

  La proprietà abilita un dato numero di stream per l'invio e la ricezione di un flusso di dati corrispondente al valore specificato, e può essere utilizzata con l'utilità di pianificazione larghezza di banda. (a pagina 237)

  Importante. In ambienti LAN, è necessario utilizzare uno stream.

- Credenziali utente

  Consente di immettere le credenziali utente per accedere alla cartella host. Se l'utente non dispone delle autorizzazioni necessarie per accedere alla directory principale, lo scenario non verrà eseguito.

Proprietà Notifica evento

Notifica

Quando si verifica un evento, è possibile impostare il sistema per l'esecuzione di uno script, l'invio di una notifica mediante posta elettronica o la scrittura nel registro eventi di Windows.

Notifica tramite messaggio di posta elettronica

Consente di definire se inviare i dettagli di un evento tramite posta elettronica a un indirizzo specificato. Se si verificano diversi eventi immediatamente uno dopo l'altro, il sistema li aggrega, inviandone i dettagli in un solo messaggio di posta elettronica.

- **In caso di errore**: impostare l'opzione su Attivo per ricevere notifiche tramite posta elettronica quando l'applicazione rileva errori.
- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica.
- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica
- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.
- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.
- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script da eseguire ogni volta che si verificherà un evento.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando si verifica un evento.
- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script, specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA, che include i dettagli dell'evento scritti in un file di notifica. Gli argomenti immessi in questa sezione sono valori statici.

Nota: su sistemi Windows x64, non è possibile eseguire script che attivano le applicazioni con interfaccia utente.

Scrivi nel Registro eventi

Consente di scrivere gli eventi nel registro eventi di Windows.

Proprietà di gestione rapporti

Salvataggio rapporti

Immettere le impostazioni per il salvataggio dei rapporti.

Directory di rapporto

Consente di specificare la posizione di salvataggio dei rapporti.

Conservazione rapporti (giorni)

Consente di specificare il numero di giorni per i quali conservare i rapporti di replica. Il valore predefinito è Illimitato.

Notifica tramite messaggio di posta elettronica

Consente di definire se inviare i rapporti tramite posta elettronica all'indirizzo specificato.

- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica.

- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica

- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.

- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.

- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script che Arcserve RHA eseguirà ogni volta che verrà generato un rapporto.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando viene generato un rapporto.

- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA. Questo argomento definisce il percorso completo del file di rapporto generato e del relativo tipo. Gli argomenti immessi in questa sezione sono valori statici.

Nota: su sistemi Windows x64, non è possibile eseguire script che attivano le applicazioni con interfaccia utente.

Pianificazione della sincronizzazione

Quando si seleziona una modalità di replica pianificata, tale sincronizzazione verrà eseguita automaticamente su base pianificata. Dopo aver selezionato questa opzione, saranno disponibili le seguenti funzionalità di pianificazione flessibile:

- Sincronizzazione in giorni selezionati della settimana e in orari specifici di un ciclo di 24 ore.
- Sincronizzazione in periodi selezionati (ad esempio, ogni 36 ore) in un ciclo di 7 giorni.
- Esclusione di date specifiche.

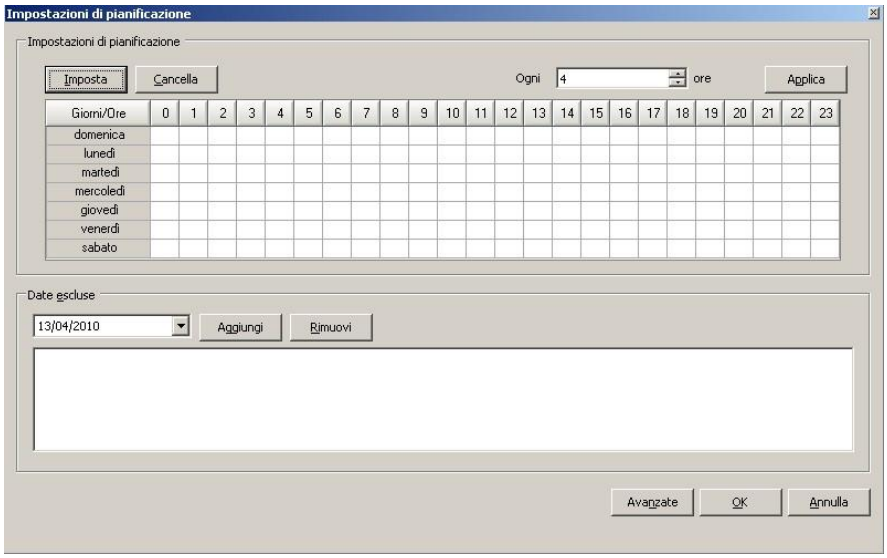
Per aprire la pianificazione, procedere come segue:

1. Nell'elenco Proprietà scenario, aprire il gruppo **Replica**. Nella proprietà **Modalità**, selezionare il valore **Pianificazione**.

   Viene visualizzata l'opzione **Pianificazione**.

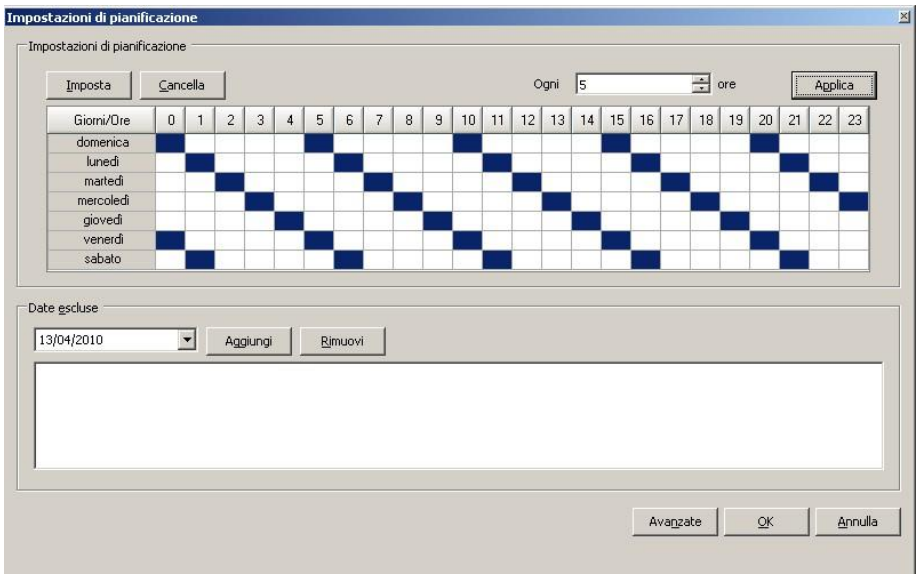
2. Nell'opzione **Pianificazione**, selezionare il valore **Attività settimanali**. Quindi, nella proprietà **Impostazioni di pianificazione**, fare clic sul valore **Non impostato**.

Viene visualizzata la finestra di dialogo **Impostazioni di pianificazione**.



3. Impostare la pianificazione per la sincronizzazione automatica in funzione delle linee guida descritte nelle sezioni seguenti.

   La figura seguente illustra un esempio di impostazione di pianificazione in cui i rettangoli di colore blu indicano i giorni e le ore pianificate per la sincronizzazione. Nell'area relativa alle date escluse sono elencate le date specifiche in cui la sincronizzazione non viene eseguita.



Impostazione di una pianificazione per la sincronizzazione automatica

Di seguito sono riportate le istruzioni per l'impostazione e la cancellazione di ore e giorni nella finestra di dialogo **Impostazioni di pianificazione** per la sincronizzazione automatica.

Per impostare un giorno/orario specifico, procedere come segue:

- Selezionare un unico rettangolo per un orario/giorno specifico. Fare clic sul pulsante **Imposta** per contrassegnare e abilitare tale orario/giorno.

Per impostare un orario specifico per ogni giorno della settimana, procedere come segue:

- Selezionare una colonna e fare clic sul pulsante **Imposta**.

Per impostare ogni ora in uno specifico giorno della settimana, procedere come segue:

- Selezionare una riga e fare clic sul pulsante **Imposta**.

Per impostare un ciclo ripetitivo, procedere come segue:

- Immettere un numero valido di ore nella casella **Ogni**, quindi fare clic sul pulsante **Applica**.

Nota: è possibile impostare più rettangoli simultaneamente facendo clic e trascinando il mouse. È anche possibile utilizzare i tasti **CTRL** e **MAIUSC** per impostare contemporaneamente più date.

Per cancellare un'impostazione, procedere come segue:

- Utilizzare la medesima tecnica adoperata per la selezione e fare clic sul pulsante **Cancella**.

Importante: se la sincronizzazione è in esecuzione e giunge l'ora della successiva sincronizzazione pianificata, la nuova sincronizzazione interrompe quella corrente e riprende dall'inizio.

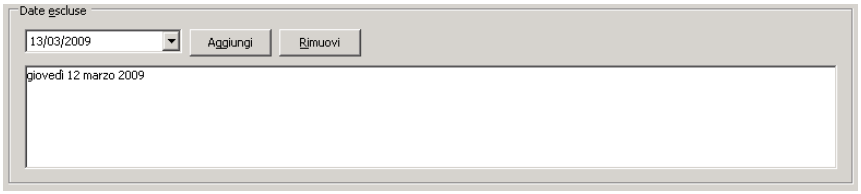
Esclusione di date dalla sincronizzazione pianificata

È possibile impostare date specifiche che saranno escluse dalla sincronizzazione automatica.

Per escludere delle date dalla sincronizzazione automatica, procedere come segue:

- Nella finestra di dialogo **Impostazioni di pianificazione**, nella sezione **Date escluse** selezionare o immettere la data esclusa nella casella **date**. Fare clic sul pulsante **Aggiungi**.

  La data selezionata viene visualizzata nell'elenco **Date escluse**.

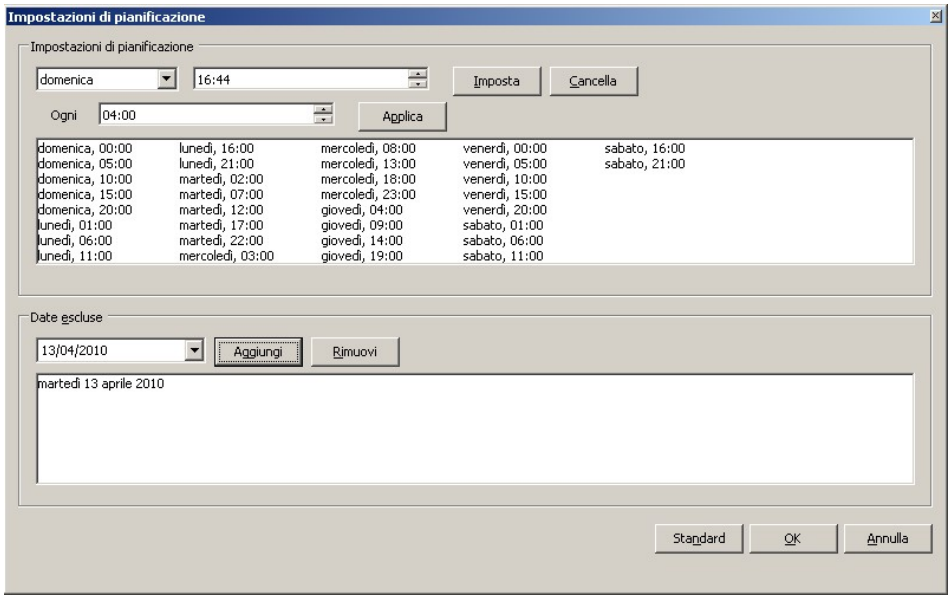


Per rimuovere una data esclusa, procedere come segue:

- Nell'elenco **Date escluse**, selezionare la data e fare clic sul pulsante **Rimuovi**. È anche possibile selezionare più date trascinando il mouse sopra di esse.

Impostazione di pianificazioni avanzate

Nella schermata **Impostazioni di pianificazione avanzata** è possibile impostare anche orari non precisi.



Per aprire la schermata Impostazione pianificazione avanzata, procedere come segue:

- Nella finestra di dialogo **Impostazioni di pianificazione**, fare clic sul pulsante **Avanzate** posto in basso.

Per tornare alla finestra di dialogo Impostazione pianificazione standard, procedere come segue:

- Nella schermata **Impostazione pianificazione avanzata**, fare clic sul pulsante **Standard** posto in basso.

Impostazione delle proprietà del server master e di replica

In questa sezione viene descritta la modalità di configurazione delle proprietà del server master e di replica, viene fornito l'elenco delle proprietà, le relative descrizioni e i valori corrispondenti.

Argomenti correlati

- Configurazione delle proprietà del server master o di replica (a pagina 216)
- Nozioni fondamentali sulle proprietà del server master (a pagina 217)
- Nozioni fondamentali sulle proprietà del server di replica (a pagina 224)
- Pianificazione del limite di larghezza di banda (a pagina 237)
- Propagazione dei valori di proprietà (a pagina 238)

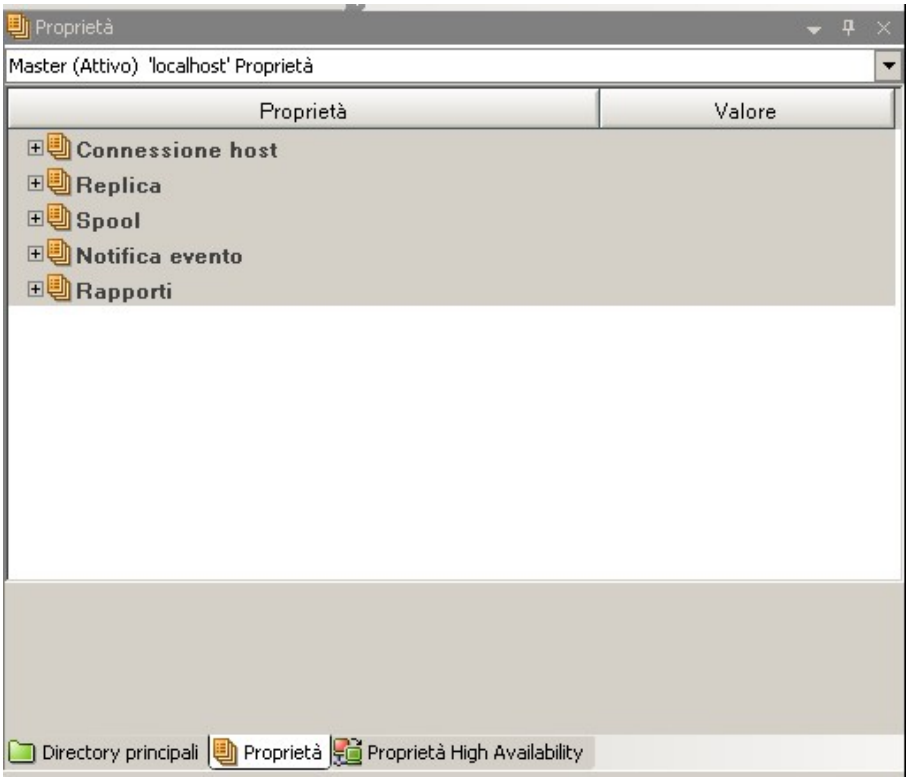
Configurazione delle proprietà del server master o di replica

Per configurare le proprietà di un server master o di replica, è necessario interrompere lo scenario.

Per impostare le proprietà del server master o di replica, procedere come segue:

1. Dal riquadro Scenario, selezionare il server master o di replica del quale si desidera configurare le proprietà.

   Nel riquadro Struttura a sinistra viene visualizzato l'elenco Proprietà di master e replica.



Nota: uno scenario in esecuzione ha lo sfondo di colore grigio, mentre gli scenari non in esecuzione hanno uno sfondo di colore bianco.

2. Se lo scenario è in esecuzione, fare clic sul pulsante **Interrompi** sulla barra degli strumenti. Lo scenario viene interrotto.
3. Nell'elenco delle proprietà del server master o di replica, aprire il gruppo desiderato, selezionare la proprietà richiesta e selezionare o immettere i valori appropriati. È possibile immettere manualmente alcuni valori nel campo di una casella di modifica mentre è possibile selezionarne altri da una casella combinata o un controllo IP facendo clic sul valore predefinito.
4. Fare clic sul pulsante **Salva** nella barra degli strumenti per salvare e applicare le proprie modifiche.

Nozioni fondamentali sulle proprietà master

In questa sezione vengono elencate le proprietà master, i valori corrispondenti, e viene fornita una spiegazione per ciascuna proprietà.

Nota: sui sistemi Windows a 64 bit, non è possibile eseguire gli script che attivano applicazioni con un'interfaccia grafica utente.

Le proprietà vengono classificate in base alla loro posizione nel relativo gruppo di proprietà:

- Connessione host (a pagina 218)
- Replica (a pagina 218)
- Spool (a pagina 220)
- Notifica di eventi (a pagina 221)
- Rapporti (a pagina 222)

Proprietà di connessione host sul Master

Indirizzo IP di gestione

Immettere l'indirizzo IP dell'host master. Se il nome del server master è stato modificato, l'indirizzo IP verrà aggiornato. È inoltre possibile modificare il server master immettendo un altro indirizzo IP in questo campo.

Indirizzo IP di replica

Immettere l'indirizzo IP di replica dell'host master. Se viene fornito l'indirizzo IP di replica, il modulo lo utilizza per trasferire i dati durante la sincronizzazione e la replica, invece dell'indirizzo IP di gestione.

Numero porta

Immettere il numero della porta in entrata utilizzata per le comunicazioni TCP. È possibile modificare il valore con una qualsiasi porta non utilizzata. Dato che il modulo può utilizzare solo una porta, assicurarsi che si tratti della porta specificata. Il numero predefinito della porta è 25000.

Configurazione del server proxy HTTP

Consente la replica dei dati mediante un server proxy HTTP. Per utilizzare un server proxy, configurare il server proxy HTTP sul master.

Proprietà di replica sul Master

Esegui script prima della sincronizzazione

Consente di attivare l'esecuzione di uno script prima di ogni sincronizzazione. Il processo di sincronizzazione non verrà avviato prima della completa esecuzione di questo script.

Nome script:

Specificare il nome e il percorso completo dello script.

Argomenti

Argomenti da passare allo script specificato nella proprietà precedente. Gli argomenti sono valori statici.

Esegui script dopo la sincronizzazione

Consente di attivare l'esecuzione di uno script dopo ogni sincronizzazione. Il processo di sincronizzazione non attenderà la completa esecuzione di questo script.

Nome script:

Specificare il nome e il percorso completo dello script.

Argomenti

Argomenti da passare allo script specificato nella proprietà precedente. Gli argomenti sono valori statici.

Comprimi dati durante il trasferimento

Consente di comprimere i dati prima di inviarli al server di replica. Questa opzione consente di ottimizzare la larghezza di banda e il tempo di trasferimento. Se l'host master è un server di produzione con traffico intenso, è consigliabile attivare questa funzione sul server di replica di primo livello che risiede sulla stessa LAN, e non sul server master.

- La compressione dei dati è un'operazione che consuma risorse e incide sulle prestazioni del server. Se il formato file tipico in corso di trasferimento non viene compresso a sufficienza, questa opzione rappresenta uno spreco di tempo ed energia. Benché sia possibile diminuire la larghezza di banda della trasmissione, il tempo di replica complessivo è una funzione di comprimibilità ed energia disponibile.
- I file già compressi quali .zip, .rar, .gz, .jpeg ecc., e qualsiasi file di dimensioni inferiori ai 512 byte, non verranno compressi.

Limitazione I/O durante la sincronizzazione

Consente di controllare la limitazione I/O durante la sincronizzazione.

Attivazione dei segnalibri pianificati (solo per scenari di database)

La proprietà consente di creare segnalibri periodici per gli scenari di database in base alla pianificazione impostata. Utilizzare i segnalibri generati nel processo di riavvolgimento per i punti di ripristino periodici. Si tratta di una funzionalità valida soltanto per gli scenari di database come MSSQL e Exchange.

Valore predefinito: ogni due ore

Esecuzione dello script alla creazione del file trigger

[Solo per file server] Consente di definire quali azioni speciali è opportuno attivare tramite uno script, quando viene specificato un file trigger.

Nome file trigger

Il nome del file che attiva lo script, specificato nella proprietà successiva. Lo script viene attivato quando si verifica l'evento di creazione del file.

Script da eseguire

- **Nome script:**

  Questo script viene richiamato quando viene creato il file trigger specificato nella proprietà precedente. Specificare il nome e il percorso completo dello script.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono essere valori statici.

Credenziali utente

Consente di immettere le credenziali utente per accedere alla cartella host. Se l'utente non dispone delle autorizzazioni necessarie per accedere alla directory principale, lo scenario non verrà eseguito.

Proprietà di spool

Lo spool è una cartella su un disco in cui vengono temporaneamente memorizzati i dati da replicare (che vengono, quindi, inseriti nello spool). Lo spool memorizza le modifiche acquisite durante la replica per un determinato periodo di tempo prima di applicarle al server di replica. I parametri di spool determinano la quantità di spazio su disco disponibile per lo spool. Nella maggior parte dei casi, il valore predefinito è sufficiente. Tuttavia, se si sceglie di modificare questo valore, impostarlo almeno sul 10% della dimensione totale del set di dati.

Dimensione max spool

Immettere la dimensione massima dello spool consentita. Questo spazio su disco verrà utilizzato solo se necessario, in quanto non è preallocato. Il valore predefinito è Illimitato. Per immettere un valore **Illimitato**, immettere zero.

Dimensione minima di spazio libero su disco

Immettere la soglia minima di spazio libero su disco raggiunta la quale il sistema genera un errore e interrompe la replica.

Directory di spool

Immettere la directory da utilizzare per memorizzare lo spool. La directory predefinita è *INSTALLDIR/tmp* in Windows.

Importante: Se si modifica il percorso di spool, ricordarsi di eliminare il nuovo percorso dalle scansioni antivirus a livello di file, sia pianificate che in tempo reale.

Proprietà Notifica evento

Notifica

Quando si verifica un evento, è possibile impostare il sistema per l'esecuzione di uno script, l'invio di una notifica tramite posta elettronica o la scrittura nel registro eventi di Windows.

Notifica tramite messaggio di posta elettronica

Consente di definire se inviare i dettagli di un evento tramite posta elettronica a un indirizzo specificato. Se si verificano diversi eventi immediatamente uno dopo l'altro, il sistema li aggrega, inviandone i dettagli in un solo messaggio di posta elettronica.

- **In caso di errore**: impostare l'opzione su Attivo per ricevere notifiche tramite posta elettronica quando l'applicazione rileva errori.
- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica.
- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica
- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.
- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.
- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script che Arcserve RHA eseguirà ogni volta che verrà inviato un rapporto.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando si verifica un evento.

- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script, specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA, che include i dettagli dell'evento scritti in un file di notifica. Gli argomenti immessi in questa sezione sono valori statici.

Scrivi nel Registro eventi

Consente di scrivere gli eventi nel registro eventi di Windows.

Proprietà rapporti

Genera rapporto di sincronizzazione

Specifica la generazione di un rapporto di sincronizzazione.

Genera rapporto dettagliato

Specifica la generazione di un rapporto di sincronizzazione dettagliato.

Genera rapporto di replica

Specifica la generazione di un rapporto di replica. Poiché il processo di replica è continuo, specificare la frequenza della generazione dei rapporti nella proprietà riportata di seguito.

Frequenza di generazione (ore)

Specifica la frequenza di generazione di un rapporto di replica.

Genera rapporto dettagliato

Specifica la generazione di un rapporto di replica dettagliato.

Gestione rapporti

Notifica tramite messaggio di posta elettronica

Specifica se inviare i rapporti tramite posta elettronica all'indirizzo specificato.

- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica**.**

- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica

- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.

- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.

- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script che Arcserve RHA eseguirà ogni volta che verrà inviato un rapporto.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando viene generato un rapporto.

- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA. Questo argomento definisce il percorso completo del file di rapporto generato e del relativo tipo. Gli argomenti immessi in questa sezione sono valori statici.

Nozioni fondamentali sulle proprietà del server di replica

In questa sezione vengono elencate le proprietà del server di replica, i valori corrispondenti, e viene fornita una spiegazione per ciascuna proprietà.

Nota: sui sistemi Windows a 64 bit, non è possibile eseguire gli script che attivano applicazioni con un'interfaccia grafica utente.

Le proprietà vengono classificate in base alla loro posizione nel relativo gruppo di proprietà:

- Connessione host
- Replica
- Computer virtuale
- Spool
- Cloud
- Recupero
- Proprietà di gestione della snapshot del volume (a pagina 233)
- Attività pianificate
- Notifica di eventi
- Rapporti

Argomenti correlati:

- Configurazione delle proprietà del master o della replica

Proprietà di connessione host sulla Replica

Indirizzo IP di gestione

Immettere l'indirizzo IP dell'host di replica. Se il nome del server di replica è stato modificato, l'indirizzo IP verrà aggiornato. È inoltre possibile modificare il server di replica immettendo un altro indirizzo IP in questo campo.

Indirizzo IP di replica

Immettere l'indirizzo IP di replica dell'host di replica. Se viene fornito l'indirizzo IP di replica, il modulo lo utilizza per trasferire i dati durante la sincronizzazione e la replica, invece dell'indirizzo IP di gestione.

Numero porta

Immettere il numero della porta utilizzata per le comunicazioni TCP. Non è possibile modificarlo con quello di una porta inutilizzata. Dal momento che il modulo può utilizzare una sola porta, assicurarsi che il modulo utilizzi la porta qui specificata. Il numero predefinito della porta è 25000.

Attivazione del server proxy HTTP

Consente la replica dei dati mediante un server proxy HTTP. Per utilizzare un server proxy, configurare il server proxy HTTP sul master.

Proprietà di replica sulla Replica

Esegui script prima della sincronizzazione

Consente di attivare l'esecuzione di uno script prima di ogni sincronizzazione. Il processo di sincronizzazione non verrà avviato prima della completa esecuzione di questo script.

Nome script:

Specificare il nome e il percorso completo dello script.

Argomenti

Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti sono valori statici.

Esegui script dopo la sincronizzazione

Consente di attivare l'esecuzione di uno script dopo ogni sincronizzazione. Il processo di sincronizzazione non attenderà il completamento dell'esecuzione dello script.

Nome script:

Specificare il nome e il percorso completo dello script.

Argomenti

Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti sono valori statici.

Comprimi dati durante il trasferimento

Consente di comprimere i dati prima di inviarli al server di replica. Questa opzione consente di ottimizzare la larghezza di banda e il tempo di trasferimento.

- La compressione dei dati è un'operazione che consuma risorse e incide sulle prestazioni del server. Se il formato file tipico in corso di trasferimento non viene compresso a sufficienza, questa opzione rappresenta uno spreco di tempo ed energia. Benché sia possibile diminuire la larghezza di banda della trasmissione, il tempo di replica complessivo è una funzione di comprimibilità ed energia disponibile.
- I file già compressi quali .zip, .rar, .gz, .jpeg ecc., e qualsiasi file di dimensioni inferiori ai 512 byte, non verranno compressi.

Crittografa i dati durante il trasferimento

Consente di eseguire la crittografia dei dati per assicurare il trasferimento protetto degli stessi tra la replica e il nodo principale corrispondente (denominato anche Comunicazione protetta). Questa proprietà può essere impostata solo sull'host di replica e non è disponibile sul master. Tuttavia, durante il recupero o l'esecuzione di scenari precedenti, questa opzione viene modificata per garantire il collegamento protetto tra i due host (o non protetto per i dati normali, se l'opzione è impostata su Nessuna crittografia).

Nota: consultare la sezioneModifica della modalità di protezione del modulo (a pagina 228) per personalizzare i parametri di protezione per la crittografia dei dati.

Conserva i file eliminati durante la sincronizzazione

Durante la sincronizzazione, non rimuovere dal server di replica i file che sono stati eliminati sul server master. È l'opzione adeguata per i casi in cui diversi scenari utilizzano le stesse directory di replica.

Conserva i file eliminati durante la replica

Durante la replica, non rimuovere dal server di replica i file che sono stati eliminati sul server master.

Limite larghezza di banda (Kbps)

Consente di controllare le dimensioni della larghezza di banda in entrata consentita sull'host di replica. È possibile definire una dimensione massima in vigore a tutte le ore del giorno oppure specificare valori diversi per orari diversi. Il valore predefinito è **Illimitato**.

Per la descrizione dettagliata della pianificazione per la larghezza di banda, fare riferimento all'argomento Pianificazione del limite di larghezza di banda (a pagina 237).

Interrompi database in esecuzione

Se questa opzione è attiva, nel caso in cui sia in esecuzione uno scenario di database (Exchange, SQL, Oracle) e il database venga eseguito sul server di replica, Arcserve RHA interrompe i servizi di database prima di eseguire lo scenario. [Non si applica agli scenari HA]

Archivia stato del sistema su questa replica

È possibile abilitare questa opzione solo quando la proprietà **Protezione stato del sistema** è attivata nell'elenco Proprietà scenario. Per ulteriori informazioni, fare riferimento all'argomento Protezione dello stato del sistema (a pagina 241).

Riprova se il file è occupato

Queste opzioni sono pertinenti solo ai server Windows. Se sono state ricevute modifiche per un file occupato (aperto come non condiviso per la lettura), queste opzioni definiscono la frequenza e l'intervallo dei tentativi di sostituzione di questo file con quello che contiene le modifiche.

Numero di tentativi

Immettere il numero di tentativi di sostituzione di un file modificato in stato occupato (e che pertanto non può essere replicato). Se il file non viene rilasciato prima che venga effettuato l'ultimo tentativo, la modifica verrà persa e verrà generato un messaggio di errore.

Intervallo tra i tentativi (msec)

Il tempo di attesa intercorso tra un tentativo vano e il tentativo successivo.

Esecuzione dello script alla creazione del file trigger

[Solo per file server] Consente di definire quali azioni speciali è opportuno attivare tramite uno script, quando viene specificato un file trigger.

Nome file trigger

Immettere il nome del file che attiva lo script, specificato nella proprietà successiva. Lo script viene attivato quando si verifica l'evento di creazione del file.

Script da eseguire

- **Nome script:**

  Questo script viene richiamato quando il file trigger specificato nella proprietà precedente viene creato. Specificare il nome e il percorso completo dello script.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono essere valori statici.

Credenziali utente

Consente di immettere le credenziali utente per accedere alla cartella host. Se l'utente non dispone delle autorizzazioni necessarie per accedere alla directory principale, lo scenario non verrà eseguito.

Modifica del metodo di protezione del modulo

Il modulo Arcserve RHA utilizza un metodo di protezione predefinito. Tuttavia, se la proprietà di replica Crittografa i dati durante il trasferimento viene impostata su *Attivo* è possibile modificare il certificato autofirmato SSL predefinito, la chiave privata RSA e l'elenco di crittografia per utilizzare i parametri di protezione personalizzati nel file di configurazione del modulo. Il file di configurazione del modulo contenente il metodo di protezione è **ws_rep.cfg**.

Per modificare il metodo di protezione del modulo

1. Interrompere l'esecuzione degli scenari che utilizzano i moduli di cui si desidera modificare il metodo di protezione, utilizzando la Gestione di Arcserve RHA.
2. Accedere all'host master di replica su cui il modulo è in esecuzione.
3. Nella finestra di dialogo Servizi, arrestare il servizio del modulo sul server master e di replica.
4. Mediante Esplora risorse, accedere alla directory di installazione del modulo, dove si trova il file ws_rep.cfg.

   Nota: La directory di installazione predefinita è la seguente: *C:\Program Files\CA\Arcserve RHA\Engine*.
5. Aprire il file ws_rep.cfg con Blocco note o un altro editor di testo.

   Nota: non è consigliabile utilizzare Blocco note, in quanto dispone di opzioni di visualizzazione limitate.
6. Eseguire le operazioni seguenti nel file ws_rep.cfg file:
   a. Individuare la sezione # SSLSelfSignedCertificate = "[INSTALLDIR]/cacert.pem".
   b. Modificare SSLSelfSignedCertificate = "[INSTALLDIR]/cacert.pem" con il nome del certificato autofirmato SSL che si desidera utilizzare, quindi rimuovere il simbolo # a inizio riga.
   c. Individuare la sezione # SSLRSAPrivateKey = "[INSTALLDIR]/cakey.pem".
   d. Modificare SSLRSAPrivateKey = "[INSTALLDIR]/cakey.pem" con il nome della chiave privata RSA che si desidera utilizzare, quindi rimuovere il simbolo # a inizio riga.
7. Salvare il file ws_rep.cfg.

   Importante. Sebbene i file di configurazione del server master e di replica possano essere diversi, verificare che i parametri utilizzati per la modifica del metodo di protezione nei file ws_rep.cfg siano identici in entrambi i server.

   Il metodo di protezione del modulo viene modificato nel file ws_rep.cfg.
8. Avviare il servizio del modulo sia sul master che sulla replica.
9. Aprire la Gestione, selezionare lo scenario ed eseguirne il riavvio.

Nota: nel caso in cui si verifichi un errore durante il caricamento del certificato autofirmato SSL e della chiave privata RSA, viene utilizzata l'impostazione predefinita e viene visualizzato un messaggio di avviso nella Gestione Arcserve RHA.

Proprietà del computer virtuale

Durante l'uso di scenari cloud, oltre alle proprietà cloud (a pagina 231), è possibile verificare e gestire le proprietà del computer virtuale:

Impostazioni della piattaforma virtuale

Consente di verificare le impostazioni delle seguenti proprietà di sola lettura:

Tipo di piattaforma virtuale

Identifica il tipo di piattaforma virtuale dell'account cloud.

Piattaforma virtuale

Identifica il server della piattaforma virtuale dell'account cloud.

Porta

Identifica il numero di porta utilizzato per la connessione al computer virtuale.

Connessione SSL

Indica se la connessione SSL (Secure Socket Layer) è attivata o disattivata.

Impostazioni del computer virtuale

Consente di definire le seguenti proprietà:

Tipo di istanza EC2

Consente di specificare la dimensione assegnata all'istanza EC2 sul computer virtuale. È possibile specificare il tipo di istanza appropriato in base al sistema operativo del server master e ai requisiti dell'ambiente in uso. Le opzioni del tipo di istanza includono:

- Istanza di piccole dimensioni
- Istanza di grandi dimensioni
- Istanza di dimensioni molto grandi
- Istanza di dimensioni molto grandi con memoria elevata
- Istanza doppia di dimensioni molto grandi con memoria elevata
- Istanza quadrupla di dimensioni molto grandi con memoria elevata
- Istanza di medie dimensioni con utilizzo elevato della CPU
- Istanza di dimensioni molto grandi con utilizzo elevato della CPU

Le opzioni disponibili fanno riferimento alla piattaforma del server master. Se il master corrisponde a un sistema operativo a 32 bit, saranno disponibili solo le istanze di piccole dimensioni e le istanze di medie dimensioni con utilizzo elevato della CPU. Se il master corrisponde a un sistema operativo a 64 bit, saranno disponibili tutti gli altri tipi di istanza.

Nome del computer virtuale

Specifica il nome del computer virtuale gestito sul server della piattaforma virtuale.

Proprietà di spool

I parametri di spool determinano la quantità di spazio su disco disponibile per lo spool. Nella maggior parte dei casi, il valore predefinito è sufficiente. Tuttavia, se si sceglie di modificare questo valore, impostarlo almeno sul 10% della dimensione totale del set di dati.

Dimensione max spool

Immettere la dimensione massima dello spool consentita. Questo spazio su disco verrà utilizzato solo se necessario, in quanto non è preallocato. Il valore predefinito è Illimitato. Per immettere un valore **Illimitato**, immettere zero.

Dimensione minima di spazio libero su disco

Immettere la soglia minima di spazio libero su disco raggiunta la quale il sistema genera un errore e interrompe la replica.

Directory di spool

Immettere la directory da utilizzare per memorizzare lo spool. La directory predefinita è *INSTALLDIR/tmp* in Windows.

Importante: Se si modifica il percorso di spool, ricordarsi di eliminare il nuovo percorso dalle scansioni antivirus a livello di file, sia pianificate che in tempo reale.

Proprietà cloud

Cloud include le seguenti proprietà:

Fornitore cloud

Specifica il nome del servizio cloud che esegue l'istanza cloud selezionata. Questa proprietà è di sola lettura.

ID account cloud

Specifica l'ID dell'account AWS. Questa proprietà è di sola lettura.

Area cloud

Specifica la regione VPC dell'account AWS. Questa proprietà è di sola lettura.

ID dell'istanza cloud

Specifica l'ID dell'istanza cloud. Questa proprietà è di sola lettura.

Pulizia delle risorse cloud durante la rimozione dello scenario

Consente di specificare se si desidera eliminare le risorse cloud in seguito alla rimozione di uno scenario. In caso di scenari High Availability per sistemi completi EC2 e scenari di replica dei dati, è possibile utilizzare diverse risorse cloud, quali l'istanza cloud utilizzata per il failover, i volumi e le snapshot. Se non è possibile utilizzare tali risorse in seguito alla rimozione dello scenario, abilitare questa opzione per eliminare le risorse cloud. Questa opzione è disattivata per impostazione predefinita.

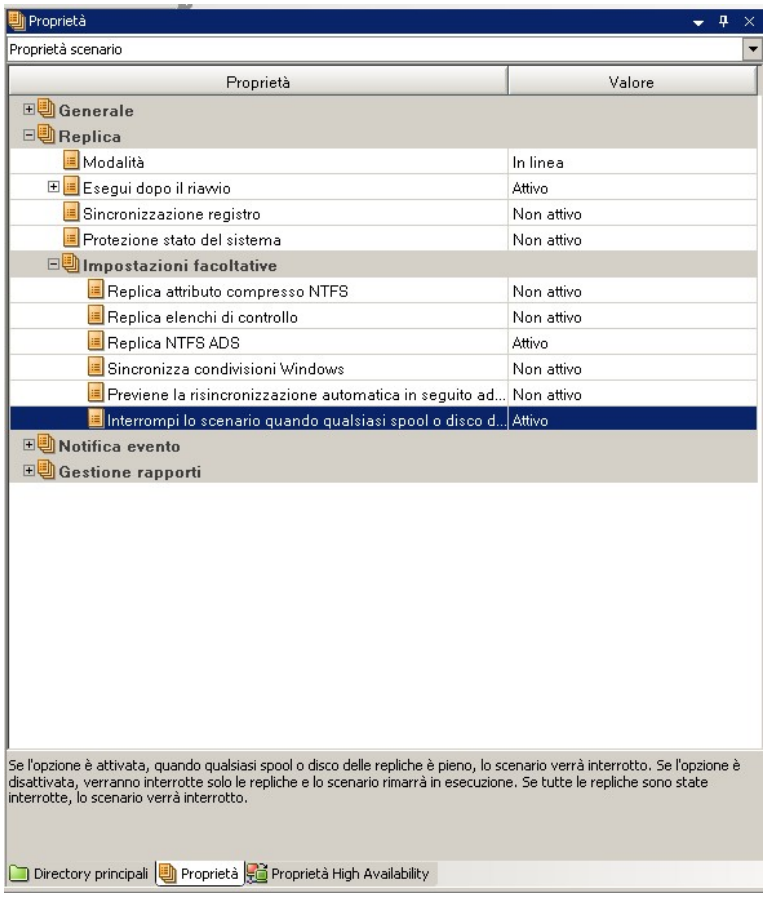
Arresta istanza quando lo scenario viene interrotto

Consente di specificare se l'istanza di replica deve essere arrestata automaticamente nel caso in cui lo scenario venga interrotto. Questa opzione è disattivata per impostazione predefinita In questo caso l'istanza di replica non verrà arrestata automaticamente in caso di interruzione dello scenario.

Modalità di interruzione di uno scenario quando lo spool è pieno

Se si dispone di scenari configurati con server di replica multipli, la proprietà che consente di interrompere lo scenario quando lo spool/il disco della replica è pieno, permette di scegliere se procedere interrompendo solo la replica interessata oppure l'intero scenario. Il valore predefinito è Attivo. Tale valore determina l'interruzione dell'intero scenario quando lo spool o il disco della replica sono pieni. Quando questa proprietà è impostata su Non attivo, viene interrotta solo la replica. Nessuna modifica verrà, quindi, inviata alla replica fino a quando questa non verrà ripresa. A quel punto, la risincronizzazione avverrà solo per la replica interessata.

Impostare la proprietà dal gruppo Replica, Impostazioni facoltative nella scheda Proprietà scenario.



Nel riquadro Eventi della Gestione, i registri di Arcserve RHA riportano che il limite di spool è stato superato oppure che lo spazio su disco è quasi esaurito. A seconda di come è stata impostata la proprietà, lo scenario o la replica vengono interrotti, consentendo di liberare spazio su disco. Lo spool viene, quindi, automaticamente ripulito.

Per avviare una replica interrotta, selezionarla facendo clic con il tasto destro del mouse dalla Gestione e scegliere di avviare la replica dal menu di scelta rapida. La risincronizzazione verrà attivata e la replica riprenderà al completamento di questa.

Proprietà di ripristino

Ritardo di replica

La replica dei dati può essere ritardata nello spool del server di replica prima di inviarla alla replica. Si tratta di una procedura utile a prevenire dati danneggiati o virus, che consente di interrompere la replica prima che dati danneggiati o infetti vengano scritti sul server di replica.

Intervallo di ritardo (min)

Immettere il numero di minuti per il ritardo della replica.

Ripristino dei dati

Conserva le informazioni di annullamento necessarie al recupero dei dati da una certa azione o da un determinato punto nel tempo. È utile nei casi in cui i dati danneggiati presenti sul server master siano stati replicati sul server di replica e si desideri ripristinare lo stato precedente dei dati, prima che venissero danneggiati. Il ripristino dati è abilitato solo per la replica in linea.

Periodo conservazione (min)

Le operazioni di I/O vengono registrate nel diario di ripristino per il numero di minuti indicato, quindi verranno eliminate a cominciare dalla prima operazione registrata.

Spazio massimo su disco (MB)

Immettere lo spazio massimo su disco allocato per il diario di ripristino. Quando questa dimensione viene raggiunta, i vecchi record vengono eliminati a cominciare dal più obsoleto.

Gestione snapshot del volume

Immettere il numero di snapshot che si desidera mantenere, il volume di archiviazione e la dimensione di archiviazione massima.

Proprietà delle attività pianificate

Sospendi

Fare riferimento all'argomento Pianificazione della sospensione della replica (a pagina 150)

Verifica di integrità di replica per Assured Recovery

Fare riferimento all'argomento Impostazione delle proprietà Assured Recovery.

Proprietà Notifica evento

Notifica

Quando si verifica un evento, è possibile impostare il sistema per l'esecuzione di uno script, l'invio di una notifica mediante posta elettronica o la scrittura nel registro eventi di Windows.

Notifica tramite messaggio di posta elettronica

Consente di definire se inviare i dettagli di un evento tramite posta elettronica a un indirizzo specificato. Se si verificano diversi eventi immediatamente uno dopo l'altro, il sistema li aggrega, inviandone i dettagli in un solo messaggio di posta elettronica.

- **In caso di errore**

  Impostare questa proprietà su Attivo per ricevere notifiche di posta elettronica quando l'applicazione rileva errori.

- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica.

- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica

- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.

- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.

- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script che Arcserve RHA eseguirà ogni volta che verrà inviato un rapporto.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando si verifica un evento.

- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script, specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA, che include i dettagli dell'evento scritti in un file di notifica. Gli argomenti immessi in questa sezione sono valori statici.

Scrivi nel Registro eventi

Consente di scrivere gli eventi nel registro eventi di Windows.

Proprietà rapporti

Genera rapporto di replica

Specifica la generazione di un rapporto di replica. Poiché il processo di replica è continuo, specificare la frequenza della generazione dei rapporti nella proprietà riportata di seguito.

Frequenza di generazione (ore)

Specifica la frequenza di generazione di un rapporto di replica.

Genera rapporto dettagliato

Specifica la generazione di un rapporto di replica dettagliato.

Genera rapporto di Assured Recovery

Specifica la generazione di un rapporto di Assured Recovery.

Gestione rapporti

Notifica tramite messaggio di posta elettronica

Specifica se inviare i rapporti tramite posta elettronica all'indirizzo specificato.

- **Server di posta elettronica**

  Immettere il nome host o l'indirizzo IP del server di posta elettronica**.**

- **Porta del server di posta elettronica**

  Immettere il numero di porta per il server di posta elettronica

- **Impostazioni di autenticazione**

  Selezionare questa opzione per aprire la finestra di dialogo Impostazioni di autenticazione di posta elettronica e immettere dettagli di autenticazione quali il nome utente, la password e le impostazioni di proxy.

- **Indirizzo di posta elettronica - A**

  Immettere l'indirizzo di posta elettronica del destinatario.

- **Indirizzo di posta elettronica - Da**

  Immettere l'indirizzo di posta elettronica del mittente.

Esegui script

Consente di specificare uno script che Arcserve RHA eseguirà ogni volta che verrà inviato un rapporto.

- **Nome script (percorso completo)**

  Immettere il nome e il percorso completo dello script che viene richiamato quando viene generato un rapporto.

- **Argomenti**

  Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Qualsiasi argomento immesso segue l'argomento inviato automaticamente da Arcserve RHA. Questo argomento definisce il percorso completo del file di rapporto generato e del relativo tipo. Gli argomenti immessi in questa sezione sono valori statici.

Pianificazione del limite di larghezza di banda

Arcserve RHA consente di monitorare le dimensioni della larghezza di banda in entrata consentita sull'host di replica. Per ogni giorno della settimana, è possibile definire una dimensione massima in vigore a tutte le ore del giorno oppure specificare valori diversi per orari diversi. Utilizzando l'Utilità di pianificazione larghezza banda, è possibile ridurre le dimensioni della larghezza di banda negli orari più intensi e aumentarla negli orari in cui il traffico è inferiore, in modo da ottimizzare le risorse disponibili.

È possibile optare anche per una sincronizzazione non in linea. Per ulteriori informazioni, consultare la sezione Metodi di sincronizzazione (a pagina 18).

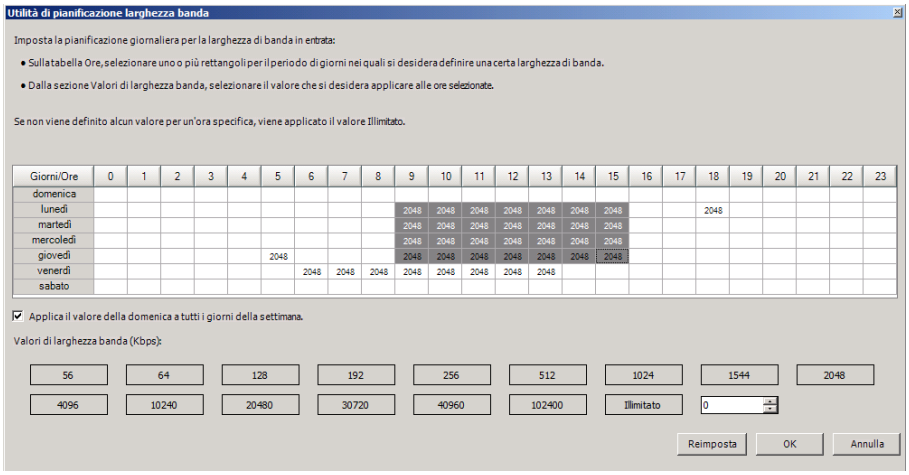
Note:

- Il limite della larghezza di banda impostato per l'host di replica non è valido anche per altri host di replica che risiedono nella stessa struttura di replica. È necessario modificare le definizioni per ciascun host di replica separatamente.
- Il valore predefinito per l'opzione Limite larghezza di banda è "**Illimitato**". Di conseguenza non viene imposta alcuna restrizione sulla larghezza di banda tra server master e server di replica.

Per pianificare il limite di larghezza di banda, procedere come segue:

1. Nell'elenco Proprietà di replica, aprire il gruppo **Replica**. Nella proprietà **Limite larghezza di banda**, fare clic sulla casella Valore in cui è impostato il valore predefinito **Illimitato**.

   Viene visualizzata la finestra di dialogo **Utilità di pianificazione larghezza banda**.


Utilità di pianificazione larghezza banda
Imposta la pianificazione giornaliera per la larghezza di banda in entrata:
• Sulla tabella Ore, selezionare uno o più rettangoli per il periodo di giorni nei quali si desidera definire una certa larghezza di banda.
• Dalla sezione Valori di larghezza banda, selezionare il valore che si desidera applicare alle ore selezionate.
Se non viene definito alcun valore per un'ora specifica, viene applicato il valore Illimitato.
Giorni/Ore 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
domenica
lunedì 2048 2048 2048 2048 2048 2048 2048 2048
martedì 2048 2048 2048 2048 2048 2048 2048 2048
mercoledì 2048 2048 2048 2048 2048 2048 2048 2048
giovedì 2048 2048 2048 2048 2048 2048 2048 2048
venerdì 2048 2048 2048 2048 2048 2048 2048 2048
sabato
Applica il valore della domenica a tutti i giorni della settimana.
Valori di larghezza banda (Kbps):
56 64 128 192 256 512 1024 1544 2048
4096 10240 20480 30720 40960 102400 Illimitato 0
Reimposta OK Annulla

2. Impostare la pianificazione giornaliera per la larghezza di banda in entrata in base alle seguenti linee guida.

   - Nella tabella **Giorni/Ore**, selezionare uno o più rettangoli corrispondenti ai momenti della giornata in cui si desidera definire una determinata larghezza di banda.

     Nota: è possibile impostare più rettangoli simultaneamente mediante la funzionalità di trascinamento del mouse. È anche possibile utilizzare i tasti **CTRL** e **MAIUSC** per impostare contemporaneamente più date.

   - Una volta contrassegnati i rettangoli, nella sezione **Valori di larghezza banda** fare clic sui valori (in Kbps) che si desidera applicare agli orari selezionati.

     I rettangoli relativi agli orari selezionati conterranno il valore impostato.

3. Per applicare una larghezza di banda a tutti i giorni, applicarla alla domenica, quindi selezionare **Applica il valore della domenica a tutti i giorni della settimana** oppure ripetere il processo per tutte le ore. Se non viene definito alcun limite per un orario specifico, verrà applicato il valore predefinito **Illimitato**.

   Nota: per cancellare l'impostazione, selezionare il pulsante **Reimposta**.

4. Al completamento delle impostazioni dell'Utilità di pianificazione larghezza banda, fare clic su **OK** per salvare le modifiche e chiudere la finestra di dialogo.

   Le impostazioni definite vengono ora visualizzate nella casella **Limite larghezza di banda** nell'elenco Proprietà:

5. Per salvare le impostazioni, fare clic sul pulsante **Salva** nella barra degli strumenti standard.

Propagazione dei valori delle proprietà

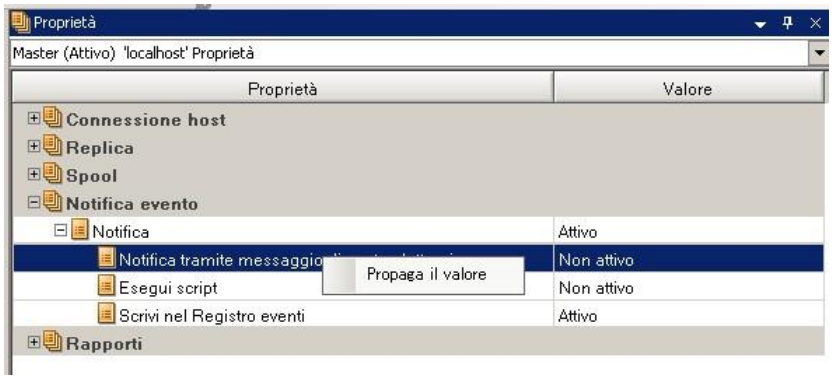
Arcserve RHA consente di applicare i valori impostati per uno scenario a più scenari contemporaneamente. Anziché configurare separatamente le proprietà per ogni singolo scenario, è possibile propagare il valore di ogni scenario a tutti gli scenari desiderati. Un ottimo esempio in questo senso consiste nell'utilizzare questa opzione per modificare contemporaneamente l'indirizzo di notifica tramite posta elettronica per più scenari. È possibile propagare i valori degli scenari, nonché host master e di replica.

Nota: per applicare le modifiche delle proprietà, gli scenari devono essere arrestati.

Per propagare i valori delle proprietà, procedere come segue:

1. Nel riquadro Scenario, selezionare lo scenario oppure l'host master o di replica di cui si desidera propagare le proprietà. Nel riquadro Struttura a sinistra viene visualizzato l'elenco Proprietà.

2. Nell'elenco Proprietà, aprire il gruppo desiderato, quindi fare clic con il tasto destro del mouse sul valore della proprietà che si desidera propagare. Viene visualizzato il comando **Propaga il valore**.



3. Fare clic sul comando **Propaga il valore**. Viene visualizzata la finestra di dialogo **Propaga il valore**.

   In questa finestra di dialogo vengono visualizzati tutti gli scenari presenti in Gestione, mentre lo scenario selezionato per la propagazione del valore della proprietà apparirà in rosso. La proprietà e il valore che è possibile propagare sono visualizzati sopra la tabella **Scenari** e nella colonna **Valore corrente**.

4. Per propagare il valore a tutti gli scenari, fare clic su **OK**.

   Nota: per escludere scenari o host dalla propagazione del valore, deselezionare le relative caselle di controllo e fare clic su **OK**.

5. Una volta chiusa la finestra di dialogo **Propaga valore**, fare clic sul pulsante **Salva tutto** sulla barra degli strumenti standard per salvare e applicare le modifiche a tutti gli scenari.

Modifica della configurazione durante l'esecuzione di uno scenario

È possibile modificare determinate proprietà durante l'esecuzione dello scenario. In tal modo è possibile risolvere i problemi senza dovere interrompere la replica.

- Proprietà di spool
  - Dimensione max spool
  - Dimensione minima di spazio libero su disco
  - Directory di spool
- Proprietà di script
  - Nome script:
  - Argomenti
- Proprietà Funzionante
  - Timeout della verifica di funzionamento
  - Frequenza heartbeat
- Limite larghezza di banda
- Limitazione I/O durante la sincronizzazione
- Proprietà di pianificazione
  - Frequenza replica periodica
  - Frequenza di generazione dei rapporti di replica
  - Modalità, pianificazione e impostazioni di pianificazione
  - Sincronizzazione del registro e frequenza di sincronizzazione
- Proprietà Notifica evento
  - Notifica tramite messaggio di posta elettronica: In caso di errore, Server di posta elettronica, Indirizzo di posta elettronica del mittente, Indirizzo di posta elettronica del destinatario
  - Esegui script
  - Scrivi nel Registro eventi

La Gestione di Arcserve RHA consente di modificare tali proprietà.

1. Dall'elenco degli scenari, fare clic sul server che si desidera configurare.
2. Fare clic sulla scheda Proprietà e ricercare la proprietà che si desidera modificare.
3. Impostare il nuovo valore in base alle proprie esigenze.

4. Fare clic su Applica, Ignora modifiche o Annulla in base alle proprie esigenze. Fare clic su Dettagli modifica per espandere la finestra di dialogo e visualizzare i valori originali e i valori nuovi delle proprietà modificate.

Durante la modifica, la freccia verde (utilizzata per indicare uno scenario in esecuzione) si converte in un'icona a forma di matita indicante la modalità di modifica. Arcserve RHA distribuisce i file di scenario modificati agli host partecipanti e verifica le modifiche. Se un host non è in grado di ricevere il file o si produce un errore di verifica, le modifiche non verranno applicate.

Protezione dello stato del sistema

La funzione Protezione stato del sistema consente di includere i componenti critici del sistema negli scenari di replica e HA, in modo da poterli ripristinare in seguito a guasti. Questa funzione è indipendente dal tipo di server in uso, ovvero è possibile abilitarla in qualsiasi scenario di Arcserve RHA. Se la funzione Protezione stato del sistema è abilitata, le informazioni sulla pianificazione delle snapshot e sulla gestione dei file vengono archiviate direttamente nel file di configurazione dello scenario. Nel caso in cui è abilitata anche la proprietà relativa alla conservazione delle snapshot di sistema (percorso di trasferimento), i file delle snapshot vengono quindi trasferiti a tutti i server di replica configurati per il server master, inclusi eventuali server di replica "figli".

Nota: anche se la proprietà di conservazione delle snapshot di sistema è abilitata sui server di replica figli ma non sul server principale, i server di replica figli non riceveranno le snapshot sullo stato del sistema.

La funzione Protezione stato del sistema consente di:

- configurare la funzione nella Creazione guidata scenario;
- impostare intervalli periodici di backup;
- inviare il file della snapshot a più server di replica;
- rieseguire il ripristino da una snapshot dello stato del sistema.

I seguenti componenti sono sempre inclusi quando la funzione Protezione stato del sistema è abilitata.

- File di avvio
- Database di registrazione classe COM+
- Servizio registro

I seguenti componenti sono inoltre inclusi nella Protezione stato del sistema a seconda del sistema operativo in uso.

- Sistemi operativi Windows Server 2003
  - Tutti i file protetti da Protezione file Windows
  - Configurazioni con monitoraggio delle prestazioni
  - Active Directory (ADSI) su sistemi che fungono da controller di dominio
  - Directory SYSVOL replicata dal servizio Replica file su sistemi che fungono da controller di dominio
  - Server certificato su sistemi con Autorità di certificazione
  - Database cluster su sistemi che fungono da nodo di un cluster Windows
- Sistemi operativi Windows Server 2008
  - Database di Servizi certificati
  - Servizi di dominio Active Directory (NTDS)
  - Directory SYSVOL directory (writer di Replica file)
  - Informazioni sul servizio cluster
  - Meta- directory di Microsoft Internet Information Services (IIS) - (Writer IIS Metabase/Writer Configurazione IIS)
  - File di sistema protetti da Protezione file Windows (Writer del sistema)

Nota: per i sistemi Windows Server 2003 o versioni successive, le snapshot di stato del sistema vengono realizzate mediante il Writer del sistema. Per ulteriori informazioni sul backup e sul ripristino dello stato del sistema mediante VSS, fare riferimento al sito Web di Microsoft.

Argomenti correlati:

- Come configurare la Protezione stato del sistema (a pagina 243)
- Modifica della protezione dello stato del sistema per lo scenario (a pagina 248)
- Ripristino dei dati relativi allo stato del sistema (a pagina 249)
- Miglioramenti della riga di comando per la protezione dello stato del sistema (a pagina 250)
- Informazioni aggiuntive sullo stato del sistema (a pagina 250)

Come configurare la Protezione stato del sistema

Per impostazione predefinita, la funzione Protezione stato del sistema è impostata su Non attivo. È possibile abilitare questa funzione durante la creazione di uno scenario mediante la procedura guidata oppure abilitarla per scenari esistenti mediante il riquadro Proprietà scenario della Gestione Arcserve RHA.

Per entrambi i metodi è necessario eseguire le operazioni seguenti.

- Abilitare la proprietà Protezione stato del sistema per lo scenario.
- Impostare la pianificazione snapshot, in base alle preferenze.
- Abilitare la proprietà Archivia protezione stato del sistema su uno o tutti i server di replica coinvolti nello scenario.

Nota: in seguito all'archiviazione dello stato del sistema su un server di replica, è necessario riavviare il computer in modo da rendere effettivo lo stato del sistema. Se necessario, è possibile attivare la proprietà Riavvia dopo il ripristino.

configurare la funzione nella Creazione guidata scenario;

È possibile attivare la Protezione stato del sistema per ciascun tipo di server supportato da Arcserve RHA, direttamente dalla Creazione guidata scenario.

Per abilitare la Protezione stato del sistema dalla procedura guidata, procedere come segue:

1. Dalla Gestione Arcserve RHA, avviare la Creazione guidata scenario utilizzando il pulsante sulla barra degli strumenti o il comando del menu Nuovo, Scenario.
2. Completare la procedura come di consueto per il tipo di server selezionato fino alla visualizzazione della finestra di dialogo Proprietà scenario.
3. In Proprietà di replica, impostare la Protezione stato del sistema su Attivo.
4. In Protezione stato del sistema, fare clic sul valore per Imposta pianificazione per accedere alla finestra di dialogo Impostazioni di pianificazione.
5. Impostare la pianificazione per la realizzazione di snapshot del sistema.
6. Completare la procedura di creazione dello scenario come di consueto, fino alla visualizzazione della finestra di dialogo Proprietà di master e replica.
7. Espandere proprietà di replica sul server di replica e impostare la proprietà Archivia stato del sistema su questa replica su Attivo. A questo punto è anche possibile impostare ulteriori proprietà di archiviazione. Per ulteriori informazioni, fare riferimento all'argomento Proprietà di archiviazione dello stato del sistema.
8. Salvare ed eseguire lo scenario. Protezione stato del sistema.

Configurazione Protezione stato del sistema per scenari esistenti

Se Protezione stato del sistema non è stata attivata durante la creazione dello scenario, è possibile configurarne l'attivazione al di fuori della creazione guidata dello scenario utilizzando la procedura indicata.

Nota: per impostazione predefinita Protezione stato del sistema è impostata su Non attivo.

Prima di eseguire questa procedura, interrompere lo scenario. Dalla Gestione Arcserve Replication, selezionare lo scenario e fare clic sul pulsante Interrompi dalla barra degli strumenti.

Per configurare la Protezione stato del sistema per scenari esistenti, procedere come segue:

1. In Gestione Arcserve Replication selezionare uno scenario per cui modificare la proprietà Protezione stato del sistema.
2. Nel riquadro Proprietà scenario, espandere il nodo Replica e impostare Protezione stato del sistema su Attivo.

   Se il server di replica non risulta configurato, verrà visualizzato un messaggio.
3. Fare clic su OK.
4. Espandere il nodo Protezione stato del sistema e impostare una pianificazione, se necessario. Per ulteriori informazioni, fare riferimento all'argomento Impostazione della Pianificazione protezione stato del sistema (a pagina 245).
5. Sul server di replica, abilitare la proprietà Archivia protezione stato del sistema. Per ulteriori informazioni, fare riferimento all'argomento Configurazione Protezione stato del sistema sul server di replica (a pagina 246).
6. Salvare lo scenario.

Ulteriori informazioni:

Impostazione della Pianificazione protezione stato del sistema (a pagina 245)
Configurazione Protezione stato del sistema sul server di replica (a pagina 246)

Impostazione della Pianificazione protezione stato del sistema

Se Protezione stato del sistema non è stata attivata durante la creazione dello scenario, è possibile configurare la proprietà Pianificazione protezione stato del sistema al di fuori della creazione guidata dello scenario utilizzando la procedura indicata.

Nota: per impostazione predefinita la Pianificazione protezione stato del sistema è impostata su Non attivo.

Per impostare la Pianificazione protezione stato del sistema, procedere come segue:

1. Dalla Gestione Arcserve RHA selezionare uno scenario per il quale impostare la proprietà di pianificazione protezione dello stato del sistema.
2. Nel riquadro Proprietà scenario, espandere il nodo Replica, quindi il nodo Protezione stato del sistema.
3. Fare clic sulla colonna Valore del nodo Imposta pianificazione.

   Viene visualizzata la finestra di dialogo Imposta pianificazione.
4. Impostare il giorno, l'ora di inizio e la frequenza, quindi escludere le date in base alle esigenze.
5. Fare clic su OK.

Configurazione Protezione stato del sistema sul server di replica

Se la Protezione stato del sistema sul server di replica non è stata abilitata durante la creazione dello scenario, è possibile configurare la proprietà Archivia stato del sistema su questa replica nella Creazione guidata scenario seguendo la procedura illustrata di seguito.

Note:

- È possibile attivare Protezione stato del sistema su più server di replica.
- Per impostazione predefinita Protezione stato del sistema è impostata su Non attivo.

Per configurare Protezione stato del sistema del server di replica, procedere come segue:

1. Dalla Gestione Arcserve RHA, selezionare un server di replica per il quale abilitare la proprietà Protezione stato del sistema.
2. Nel riquadro Proprietà, espandere il nodo Replica e impostare Archivia stato del sistema su questa replica su Attivo.
3. Modificare la proprietà di archiviazione del server di replica secondo le esigenze. Per ulteriori informazioni, fare riferimento all'argomento Proprietà di archiviazione dello stato del sistema (a pagina 247).
4. Salvare lo scenario.

Proprietà di archiviazione dello stato del sistema

È possibile impostare le seguenti proprietà sul server di replica per gestire l'archiviazione delle snapshot sullo stato del sistema.

Copie da conservare

Specificare il numero snapshot relative allo stato del sistema da conservare sul server di replica. Il valore predefinito è 8. Per un numero di snapshot illimitato, immettere il valore zero. Se il numero di snapshot supera il valore impostato, le snapshot meno recenti vengono eliminate per liberare spazio a favore delle snapshot successive.

Spazio massimo totale su disco (MB)

Specificare lo spazio totale massimo su disco da riservare alle snapshot relative allo stato del sistema.

Valori predefiniti per sistema operativo:

- Windows 2003: 8192
- Windows 2008: 16.384

Per una quantità di spazio illimitata, immettere il valore zero. Se lo spazio allocato viene interamente utilizzato dalle snapshot, le snapshot meno recenti vengono eliminate per liberare spazio a favore delle snapshot successive.

Nota: Arcserve RHA controlla le impostazioni delle opzioni Copie da conservare e Spazio massimo totale su disco periodicamente, non all'avvio dello scenario.

Spazio libero su disco minimo (MB)

Specificare lo spazio totale minimo su disco per le snapshot relative allo stato del sistema. Il valore predefinito è 1024. Se lo spazio libero sul disco è inferiore al valore impostato, le snapshot meno recenti vengono eliminate per garantire lo spazio minimo sul disco.

directory

Specificare la directory in cui archiviare le snapshot relative allo stato del sistema.

Modifica della protezione dello stato del sistema per lo scenario

Quando uno scenario viene interrotto, è possibile modificarne le proprietà inclusa la proprietà Protezione stato del sistema. Le modifiche apportate saranno effettive al riavvio dello scenario.

Proprietà Protezione stato del sistema

Se si disabilita la proprietà Protezione stato del sistema su uno scenario esistente, viene richiesto di eliminare le snapshot esistenti. Scegliere Sì, per eliminare tutte le snapshot dal server di replica al riavvio dello scenario. Scegliere No, per conservare tutte le snapshot.

Proprietà Archivia stato del sistema su questa replica

Se si disabilita la proprietà Archivia stato del sistema su questa replica su uno scenario esistente, viene richiesto di eliminare le snapshot esistenti. Scegliere Sì, per eliminare tutte le snapshot; scegliere No per conservarle.

È possibile modificare tutte le proprietà nel gruppo Archivia stato del sistema su questa replica.

Copie da conservare

È possibile impostare il numero di snapshot da conservare.

Spazio massimo totale su disco (MB)

È possibile impostare lo spazio massimo totale disponibile sul disco.

Spazio libero su disco minimo (MB)

È possibile impostare lo spazio minimo libero sul disco da allocare al salvataggio delle snapshot. Se il valore impostato corrisponde 0, lo spazio è illimitato. Se il valore impostato è inferiore allo spazio occupato durante l'esecuzione dello scenario, le snapshot meno recenti vengono eliminate per liberare spazio a favore delle nuove snapshot.

Modifica directory per archiviazione snapshot

È possibile modificare la directory in cui salvare le snapshot archiviate. Se si specifica un percorso non valido, viene visualizzato un messaggio in cui si avvisa che non è possibile salvare le snapshot. Se si specifica un percorso valido, viene richiesto di spostare le snapshot precedenti in una nuova posizione. Scegliere No, per eliminare le snapshot precedenti.

Per ulteriori informazioni, fare riferimento all'argomento Proprietà di archiviazione dello stato del sistema (a pagina 247).

Ripristino dei dati relativi allo stato del sistema

Il processo di ripristino dei dati relativi allo stato del sistema è simile al consueto processo di ripristino, con un'eccezione. Se la Protezione stato del sistema è abilitata, al momento del ripristino, viene richiesto di selezionare un'origine ripristino (vedere la procedura riportata di seguito).

Arcserve RHA attende il completamento del ripristino dei dati dell'applicazione, inclusa la sincronizzazione, prima di ripristinare lo stato del sistema. È necessario selezionare un server di replica che funga da computer di origine per il ripristino. Durante il processo di ripristino, viene creato un nuovo scenario in cui vengono invertiti i ruoli dei server master e di replica. Lo scenario trasferisce quindi la snapshot sullo stato del sistema al server master originario.

Per ripristinare i dati relativi allo stato del sistema, procedere come segue:

1. Dalla Gestione Arcserve RHA, selezionare uno scenario per il quale ripristinare i dati relativi allo stato del sistema.
2. Selezionare l'host di replica
3. Sulla barra degli strumenti, fare clic sul pulsante Ripristino dei dati

   Se la proprietà Protezione stato del sistema è abilitata per lo scenario, viene visualizzata la finestra di dialogo Origine ripristino.
4. Fare clic su Ripristina dati archiviazione e Ripristina stato del sistema, quindi fare clic su Avanti.

   Nota: se si seleziona solo Ripristina stato del sistema, non sarà possibile scegliere un punto di ripristino per l'applicazione. Se si disabilita la Protezione stato del sistema, la schermata Origine ripristino non viene visualizzata.

   Viene visualizzata la finestra di dialogo Seleziona punto di ripristino.
5. Dalla finestra di dialogo Seleziona punto di ripristino, fare clic su Seleziona punto di ripristino per aprire le finestra di dialogo Selezione punto di ripristino.
6. Impostare i seguenti criteri:

   Ora

   Selezionare un punto precedente di backup dall'elenco.

   Ripristina in

   Ripristinare i dati nella posizione predefinita o accedere a una posizione specifica.
7. Fare clic su Fine.
8. Riavviare il server di replica.

Miglioramenti della riga di comando per la protezione dello stato del sistema

I seguenti comandi sono stati aggiunti alla PowerShell per garantire il supporto per la proprietà Protezione stato del sistema.

set-properties nome_scenario index value

Utilizzare il comando set-properties per impostare la Protezione stato del sistema per uno scenario

Per ottenere i valori di indice, utilizzare il comando get-properties.

set-hostproperty nome_scenario nome_replica index value

Utilizzare il comando set-hostproperty per abilitare la Protezione stato del sistema su un server di replica.

Per ottenere i valori di indice, utilizzare il comando get-hostproperties.

RecoveryMode [A|S|B]

Utilizzare A per ripristinare solo i dati dell'applicazione (impostazione predefinita).

Utilizzare S per ripristinare solo i dati del sistema.

Utilizzare B per ripristinare entrambi.

RebootAfterRecovery [0|1]

Utilizzare 0 per evitare il riavvio (impostazione predefinita).

Utilizzare 1 per abilitare il riavvio del server master in seguito al ripristino.

Informazioni aggiuntive sullo stato del sistema

Protezione stato del sistema in scenario High Availability

In seguito a un avanzamento, le snapshot sullo stato del sistema non vengono conservate sul server master originario.

Capitolo 9: Recupero di dati e server

Questa sezione descrive le modalità di ripristino di server e dati mediante la Gestione, le modalità di impostazione dei segnalibri e di ripristino dei dati.

Questa sezione contiene i seguenti argomenti:

Processo di ripristino dei dati (a pagina 251)
Ripristino di dati perduti dal server di replica (a pagina 252)
Impostazione di segnalibri (a pagina 254)
Ripristino dei dati (a pagina 255)

Processo di ripristino dei dati

Quando un evento causa la perdita di dati del server master, è possibile ripristinarli da qualsiasi server di replica. Il processo di ripristino è un processo di sincronizzazione nella direzione inversa: dal server di replica al server master.

Arcserve RHA consente il ripristino dei dati in due modi:

- **Ripristino dei dati dal server di replica al server master** -- L'opzione è una procedura di sincronizzazione nella direzione opposta e richiede l'interruzione dello scenario. L'opzione non è consigliata per scenari Oracle, SQL o Exchange.
- **Ripristino dei dati da un determinato evento o punto nel tempo (Ripristino dati)** -- L'opzione utilizza una procedura con punti di arresto con contrassegno e segnalibri definiti dall'utente per ripristinare i dati corrotti sul server master a un momento precedente al loro danneggiamento.

Importante: per avviare il ripristino, è necessario interrompere la replica

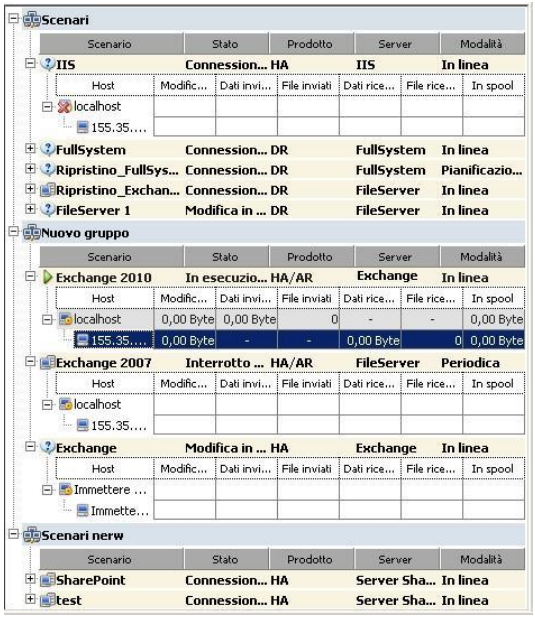
Ripristino di dati perduti dal server di replica

È possibile ripristinare dati da un server di replica. Tale operazione potrebbe richiedere credenziali di accesso per il computer utilizzato.

Per ripristinare tutti i dati perduti da un server di replica, procedere come segue:

1. Nella Gestione, dal riquadro Scenario selezionare lo scenario desiderato e interromperlo.
2. [Solo per applicazioni di database] Interrompere i servizi di database sull'host master.
3. Nella Gestione, dalla cartella dello scenario selezionare l'host del server di replica:

   Nota: se più server di replica partecipano allo scenario richiesto, selezionare il server di replica dal quale si desidera recuperare i dati.


Scenari
Scenario Stato Prodotto Server Modalità
IIS Connession... HA IIS In linea
Host Modific... Dati invi... File inviati Dati rice... File rice... In spool
localhost
155.35....
FullSystem Connession... DR FullSystem In linea
Ripristino_FullSys... Connession... DR FullSystem Pianificazio...
Ripristino_Exchan... Connession... DR FileServer In linea
FileServer 1 Modifica in ... DR FileServer In linea
Nuovo gruppo
Scenario Stato Prodotto Server Modalità
Exchange 2010 In esecuzio... HA/AR Exchange In linea
Host Modific... Dati invi... File inviati Dati rice... File rice... In spool
localhost 0,00 Byte 0,00 Byte 0 - - 0,00 Byte
155.35.... 0,00 Byte - - 0,00 Byte 0 0,00 Byte
Exchange 2007 Interrotto ... HA/AR FileServer Periodica
Host Modific... Dati invi... File inviati Dati rice... File rice... In spool
localhost
155.35....
Exchange Modifica in ... HA Exchange In linea
Host Modific... Dati invi... File inviati Dati rice... File rice... In spool
Immettere ...
Immette...
Scenari nerw
Scenario Stato Prodotto Server Modalità
SharePoint Connession... HA Server Sha... In linea
test Connession... HA Server Sha... In linea

   L'opzione **Ripristina dati** è attivata.

4. Dal menu **Strumenti** scegliere **Ripristina dati** oppure fare clic sul pulsante **Ripristina dati** sulla barra degli strumenti standard.

   Viene visualizzata la schermata **Metodo di recupero** della procedura Ripristino guidato dei dati.

Note:

- Se la proprietà **Ripristino dati** è impostata su Attivo, viene visualizzata un'altra finestra di dialogo **Ripristino dei dati**. In questo caso, selezionare la prima opzione: Sostituisci tutti i dati presenti sul server Master con i dati della replica.
- La casella di controllo **Includi sincronizzazione chiavi di registro** è abilitata solo se è stata attivata la proprietà Sincronizzazione registro (a pagina 184) prima dell'avvio dello scenario. Se la casella è disponibile, selezionarla per includere le chiavi di registro sincronizzate nel processo di ripristino.

5. Fare clic su **Avanti**. Viene visualizzata la schermata **Metodo di sincronizzazione**.
6. Selezionare il metodo di sincronizzazione appropriato in base al tipo di scenario. Fare clic su Fine.

   Nota: se le credenziali utente utilizzate per accedere alla Gestione sono diverse da quelle richieste per l'utilizzo del modulo sul server di replica, viene visualizzata la finestra di dialogo Credenziali utente, in cui viene richiesto di immettere i dettagli dell'account di accesso per il server di replica selezionato.

   Dopo aver avviato il processo di ripristino, Arcserve RHA crea una struttura inversa temporanea utilizzando il server di replica selezionato come principale e il server master come nodo finale. Al termine del processo di ripristino del server master, lo scenario temporaneo viene eliminato e nel riquadro Eventi viene visualizzato il seguente messaggio: **Sincronizzazione terminata**.
7. Per impostazione predefinita, dopo che è stato eseguito un recupero dei dati verrà generato un Rapporto di sincronizzazione.

   A questo punto, è possibile riavviare il processo di replica sullo scenario originale.

Impostazione di segnalibri

Un *segnalibro* è un punto di arresto impostato manualmente per marcare uno stato al quale è possibile eseguire il ripristino. Si consiglia di impostare un segnalibro prima di eseguire qualsiasi attività che potrebbe provocare l'instabilità dei dati. I segnalibri vengono impostati in tempo reale, non per eventi passati.

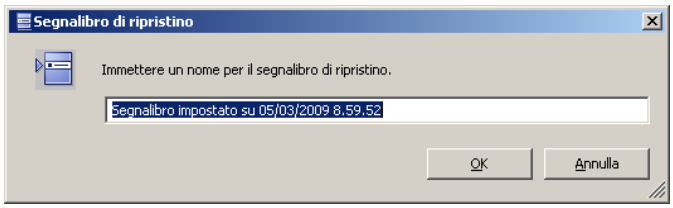
Note:

- È possibile utilizzare questa opzione solo se si imposta su *Attivo* l'opzione Ripristino - Ripristino dati (per impostazione predefinita, l'opzione è impostata su *Non attivo*).
- Non è possibile impostare segnalibri durante il processo di sincronizzazione.
- È possibile inserire segnalibri manuali per gli scenari HA per sistemi completi.

Per impostare un segnalibro, procedere come segue:

1. Selezionare l'host di replica dal riquadro Scenario da cui si desidera ripristinare i dati quando lo scenario richiesto è in esecuzione.
2. Selezionare l'opzione per l'impostazione del segnalibro di ripristino dal menu Strumenti.

   Viene visualizzata la finestra di dialogo Segnalibro di ripristino.

   Il testo visualizzato nella finestra di dialogo Segnalibro di ripristino verrà visualizzato nella finestra di dialogo di selezione dei punti di ripristino come nome del segnalibro. Il nome predefinito comprende la data e l'ora.
3. Accettare il nome predefinito oppure immettere un nuovo nome per il segnalibro, quindi fare clic su OK.

   Nota: si consiglia di attribuire un nome significativo al segnalibro per la sua futura identificazione.

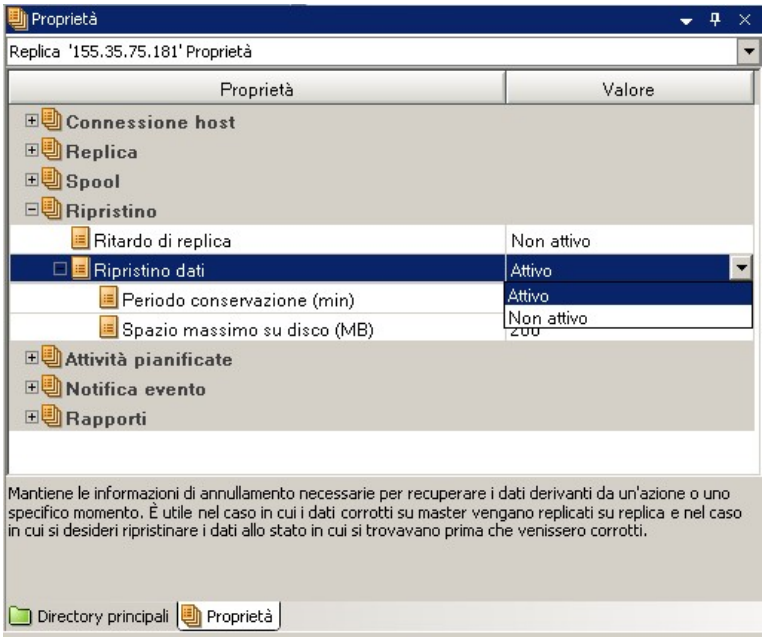
   Il segnalibro è stato impostato.

Nota: in alcuni scenari, come ad esempio in scenari HA per sistemi completi, non è possibile apportare modifiche al diario finché la creazione del segnalibro non viene completata.

Ripristino dei dati

Il metodo di recupero Ripristino dati consente il ripristino di file a un punto nel tempo precedente al loro danneggiamento. Il processo di ripristino ha luogo sul server di replica, prima che cominci il processo di sincronizzazione inversa. Il metodo Ripristino dati utilizza questi punti di ripristino o segnalibri per reimpostare i dati correnti su uno stato precedente.

È possibile utilizzare questa opzione solo se si imposta su **Attivo** l'opzione **Ripristino - Ripristino dati**.


Proprietà
Replica '155.35.75.181' Proprietà
Proprietà
Valore
Connessione host
Replica
Spool
Ripristino
Ritardo di replica
Non attivo
Ripristino dati
Attivo
Periodo conservazione (min)
Attivo
Non attivo
Spazio massimo su disco (MB)
Attività pianificate
Notifica evento
Rapporti
Mantiene le informazioni di annullamento necessarie per recuperare i dati derivanti da un'azione o uno specifico momento. È utile nel caso in cui i dati corrotti su master vengano replicati su replica e nel caso in cui si desideri ripristinare i dati allo stato in cui si trovavano prima che venissero corrotti.
Directory principali
Proprietà

Se questa opzione è impostata su Non attivo, il sistema non registrerà punti di ripristino dei dati.

Importante: Il processo di ripristino dei dati opera in una sola direzione, non è possibile quindi riprodurre scenari successivi. Al termine del ripristino, tutti i dati successivi al punto di ripristino andranno persi, poiché verranno sovrascritti da nuovi dati. Non è possibile eseguire il ripristino su un punto precedente alle modifiche apportate ai file di replica.

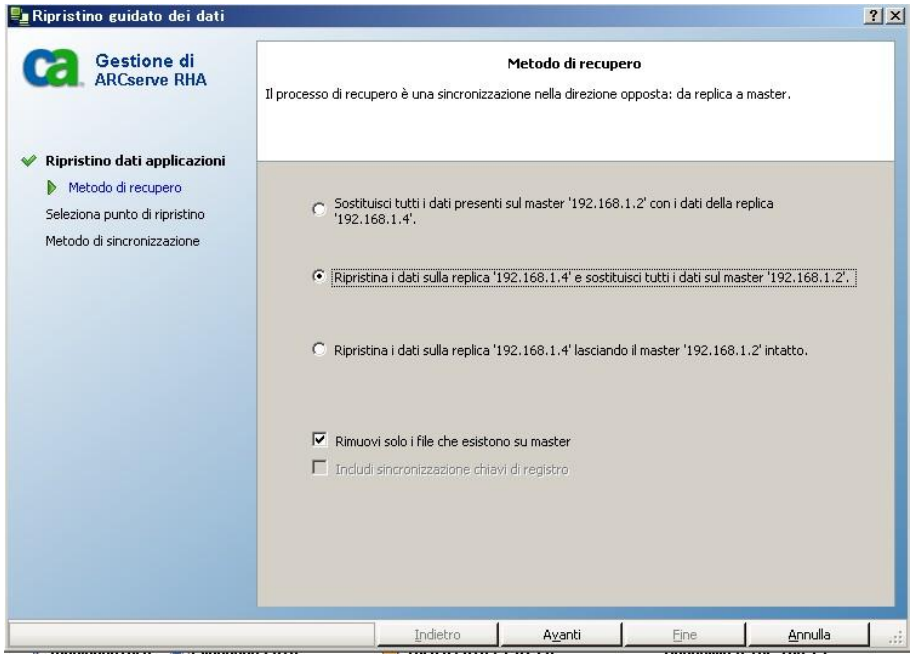
Nota: la registrazione automatica dei punti di ripristino ha inizio solo al termine del processo di sincronizzazione. Nel riquadro Evento verrà visualizzato il messaggio: **Tutte le modifiche avvenute durante il periodo di sincronizzazione sono state replicate**. Allo stesso modo, non è possibile impostare manualmente i segnalibri durante la sincronizzazione. Nel seguente esempio, viene utilizzato uno scenario file server, tuttavia la procedura resta invariata per tutti i tipi di scenario.

Per ripristinare i dati utilizzando i punti di ripristino, procedere come segue:

1. Nella Gestione, dal riquadro Scenario selezionare lo scenario desiderato e interromperlo.
2. [Solo per applicazioni di database] Interrompere i servizi di database sull'host master.
3. Nella Gestione, dalla cartella dello scenario selezionare l'host del server di replica:

   Nota: se più server di replica partecipano allo scenario richiesto, selezionare il server di replica dal quale si desidera recuperare i dati.
4. Nel menu **Strumenti**, selezionare **Ripristina dati** oppure fare clic sul pulsante **Ripristina dati**. Se vengono richieste le credenziali utente, immettere le informazioni appropriate e fare clic su OK.

   Viene visualizzata la schermata **Metodo di recupero** della procedura Ripristino guidato dei dati.


Ripristino guidato dei dati
Gestione di ARCserve RHA
Ripristino dati applicazioni
Metodo di recupero
Seleziona punto di ripristino
Metodo di sincronizzazione
Metodo di recupero
Il processo di recupero è una sincronizzazione nella direzione opposta: da replica a master.
Sostituisci tutti i dati presenti sul master '192.168.1.2' con i dati della replica '192.168.1.4'.
Ripristina i dati sulla replica '192.168.1.4' e sostituisci tutti i dati sul master '192.168.1.2'.
Ripristina i dati sulla replica '192.168.1.4' lasciando il master '192.168.1.2' intatto.
Rimuovi solo i file che esistono su master
Includi sincronizzazione chiavi di registro
Indietro
Avanti
Fine
Annulla

5. Selezionare una delle opzioni di Ripristino dati, a seconda che si desideri eseguire la sincronizzazione dei dati anche sul server master (opzione 2) oppure lasciarli solo sul server di replica (opzione 3).

   Note:

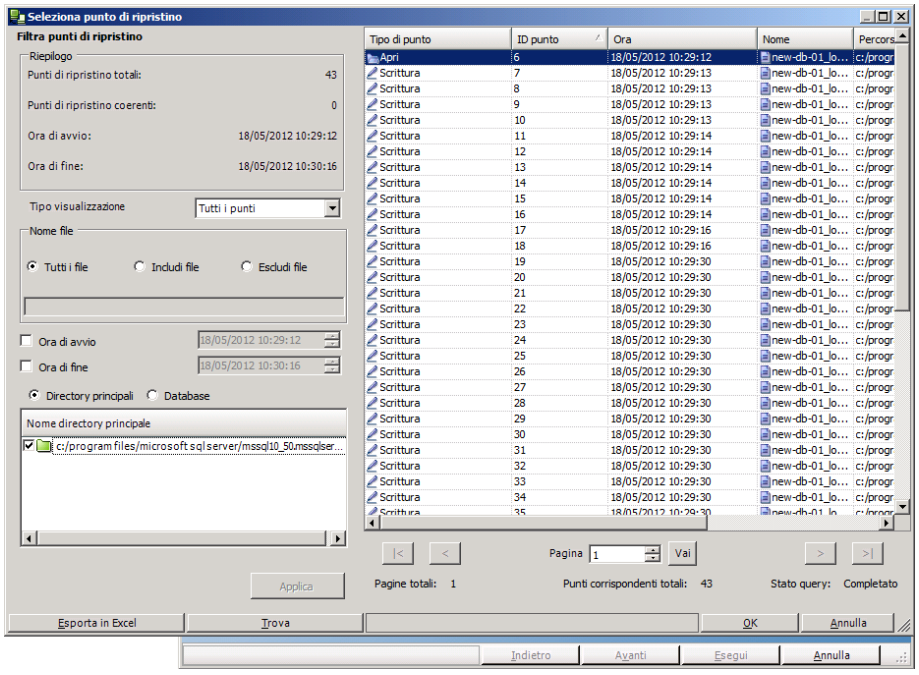
   - Se le credenziali utente utilizzate per accedere a Gestione sono diverse da quelle richieste per l'utilizzo del modulo sul server di replica, viene visualizzata la finestra di dialogo **Credenziali utente** in cui viene richiesto di immettere i dettagli dell'account di accesso per il server di replica selezionato.
   - La casella di controllo **Includi sincronizzazione chiavi di registro** è abilitata solo se è stata attivata la proprietà Sincronizzazione registro (a pagina 184) prima dell'avvio dello scenario. Se la casella è disponibile, selezionarla per includere le chiavi di registro sincronizzate nel processo di ripristino.

   Dopo aver selezionato un'opzione di ripristino dei dati, verrà creato automaticamente uno scenario di ripristino. Tale scenario rimarrà in esecuzione fino al termine del processo di ripristino.

6. Fare clic su **Avanti**. Viene visualizzata la schermata **Seleziona punto di ripristino**.

7. Attendere che il pulsante **Seleziona punto di ripristino** venga attivato, quindi fare clic su di esso per visualizzare i punti di ripristino esistenti.

   Viene visualizzata la finestra di dialogo **Seleziona punto di ripristino**.



Viene visualizzata la finestra di dialogo **Seleziona punto di ripristino** in cui presente un elenco di tutti i punti di ripristino appropriati per l'applicazione che si desidera proteggere. Tra questi sono incluse le modifiche delle cartelle e dei file che sono stati automaticamente registrati dal sistema e i segnalibri definiti dall'utente.

È possibile filtrare l'elenco in base al tipo di punto di ripristino o ad altri criteri, utilizzando il riquadro **Filtra punti di ripristino** a sinistra.

Note:

- Se la finestra di dialogo **Seleziona punto di ripristino** è vuota, assicurarsi che la proprietà Ripristino dati (a pagina 233)sia abilitata.
- È possibile esportare l'intero elenco in un file di Excel facendo clic sul pulsante **Esporta in Excel** nell'angolo in basso a destra.

8. Selezionare il punto di ripristino richiesto e fare clic su **OK.**

   Nota: se si desidera utilizzare un segnalibro come punto di ripristino, si consiglia di selezionare il punto di ripristino più vicino che indica un evento effettivo.

   Viene visualizzata nuovamente la schermata **Seleziona punto di ripristino**, che ora conterrà informazioni sul punto di ripristino selezionato.

9. Fare clic su **Avanti**. Viene visualizzata la schermata **Metodo di sincronizzazione**.

10. Selezionare il metodo di sincronizzazione appropriato e fare clic su **Fine**.

    Nota: se le credenziali utente utilizzate per accedere alla Gestione sono diverse da quelle richieste per l'utilizzo del modulo sul server di replica, viene visualizzata la finestra di dialogo **Credenziali utente**, in cui viene richiesto di immettere i dettagli dell'account di accesso per il server di replica selezionato.

    Arcserve RHA ripristina i dati al punto selezionato dall'utente. Al termine del processo di ripristino, nel riquadro Eventi verrà visualizzato il seguente messaggio: **Processo di ripristino completato correttamente**.

    Se si sceglie di sostituire i dati sul server master con i dati sul server di replica, Arcserve RHA avvia un processo di sincronizzazione dal server di replica al server master. Al termine del processo, lo scenario di ripristino temporaneo viene interrotto e quindi eliminato.

11. Per impostazione predefinita, dopo che è stato eseguito un recupero dei dati viene generato un rapporto di sincronizzazione.

    A questo punto, è possibile riavviare il processo di replica sullo scenario originale.

Capitolo 10: Avanzamento e regressione

Questa sezione illustra il processo High Availability, le procedure di avanzamento e regressione e le seguenti operazioni: creazione di uno scenario HA, esecuzione di avanzamento e regressione e recupero del server attivo.

Questa sezione contiene i seguenti argomenti:

Avanzamento (a pagina 259)
Regressione (a pagina 262)
Recupero del server attivo (a pagina 265)
Nozioni fondamentali sul sistema High Availability e sulle procedure di avanzamento e regressione (a pagina 270)
Impostazione delle proprietà High Availability (a pagina 271)

Avanzamento

Flusso di lavoro di avanzamento

L'avanzamento (o failover) è il processo di scambio dei ruoli tra server master e server di replica, in cui il primo diventa il server in stand-by e il secondo diventa il server attivo.

In Arcserve RHA è possibile attivare automaticamente l'avanzamento quando il server master risulta non disponibile (failover). In alternativa, Arcserve RHA può semplicemente avvisare l'utente del problema, di modo che questi possa avviare manualmente l'avanzamento dalla Gestione.

Durante la creazione dello scenario HA, l'utente definisce in che modo desidera avviare l'avanzamento. Se è stata selezionata l'opzione per l'avvio dell'**avanzamento manuale** nella schermata **Avvio replica inversa e di avanzamento**, eseguire un avanzamento manuale. Se è stata selezionata l'opzione **Avanzamento automatico**, è ancora possibile eseguire un avanzamento manuale, anche se il server master è funzionante. È possibile avviare l'avanzamento quando si desidera testare il sistema oppure utilizzare il server di replica per continuare il servizio di applicazione, eseguendo al contempo una determinata forma di manutenzione sul server master.

Se si sceglie di avviare l'avanzamento in modo automatico, quando il server master risulta non attivo, Arcserve RHA tenta di ripristinare automaticamente i servizi e i database su tale server con il relativo stato attivo. In un primo momento, Arcserve RHA tenta di riavviare i servizi verificati precedentemente. Quindi, se tali servizi sono in esecuzione, tenta di eseguire il montaggio dei database. Se tutti i tentativi non riescono, Arcserve RHA avvia il failover. Questi tentativi di ripristino dei servizi e del server non vengono eseguiti se l'avanzamento viene avviato manualmente.

Una volta attivato, manualmente o automaticamente, il processo di avanzamento stesso è completamente automatizzato.

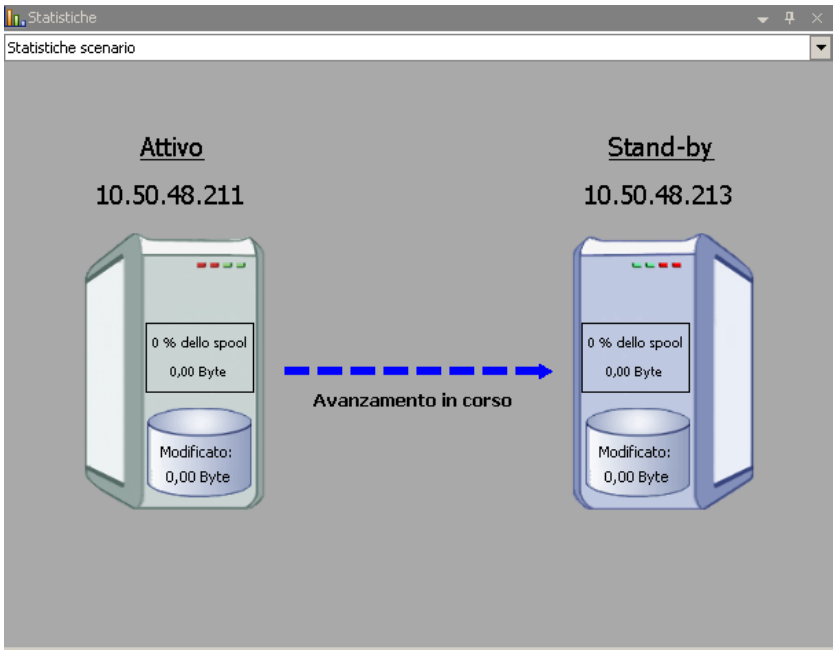
Avvio dell'avanzamento

Per avviare l'avanzamento, procedere come segue:

1. Aprire la Gestione e selezionare lo scenario desiderato dal riquadro Scenario. Verificare che lo scenario sia in esecuzione.
2. Fare clic sul pulsante **Esegui avanzamento** oppure scegliere l'opzione **Esegui avanzamento** dal menu **Strumenti**:

   Verrà visualizzato un messaggio di conferma.
3. Se lo si desidera è possibile selezionare **Non attendere fino all'applicazione di tutti i diari** per eseguire immediatamente l'avanzamento, prima del completamento dell'applicazione di tutti i diari. Se non si seleziona questa casella di controllo, il processo di avanzamento verrà avviato solamente una volta applicati tutti i diari.
4. Fare clic su Sì.

5. A seconda della configurazione dello scenario in uso, la casella di controllo **Esegui lo scenario di replica inversa dopo l'avanzamento** potrebbe essere selezionata o meno. È possibile modificare la propria configurazione predefinita solo per l'avanzamento che si sta per eseguire, selezionando o deselezionando la casella di controllo. Fare clic su **Sì**nella finestra di conferma **Esegui avanzamento**. In questo modo viene avviato un avanzamento dal server master al server di replica.



È possibile trovare informazioni dettagliate sui processi di avanzamento nel riquadro Eventi durante l'avanzamento.

6. Una volta completato l'avanzamento, lo scenario viene interrotto.

Nota: l'unico caso in cui è possibile continuare a eseguire lo scenario dopo l'avanzamento si verifica quando la **replica inversa automatica** è impostata sull'**avvio automatico**.

Nel riquadro Eventi viene visualizzato il messaggio **Avanzamento completato**, quindi **Lo scenario è stato interrotto**.

A questo punto, il server master originario diviene il server di replica, mentre il server di replica originario diviene il server master.

Importante. Se il server master subisce un arresto anomalo oppure viene riavviato durante un avanzamento, il processo viene interrotto. In tal caso, potrebbe essere necessario ripristinare il server attivo. (a pagina 265)

Regressione

Flusso di lavoro di regressione

Dopo aver avviato un avanzamento, manualmente o automaticamente, a un certo punto l'utente avrà bisogno di invertire i ruoli dei server, rendendo di nuovo attivo il server master originario e reimpostando il server di replica come server in stand-by. Prima di eseguire la regressione i ruoli, se si desidera che i dati restino sul server attivo (ossia il server di replica originario), è necessario eseguire uno scenario inverso (detto anche scenario precedente) per sovrascrivere i dati sul server in stand-by.

Durante la creazione dello scenario HA, l'utente definisce la modalità di avvio dello scenario inverso. Selezionando l'opzione che consente l'**avvio automatico della replica inversa** la replica inversa (da replica a master) viene avviata automaticamente dopo un avanzamento, non appena il master originale diventa disponibile. Se è stata selezionata l'opzione per l'**avvio manuale della replica inversa** , è necessario eseguire la regressione manualmente. Se si seleziona l'opzione manuale e non si avvia una regressione manuale, è necessario risincronizzare i dati dal server di replica al server master, anche dopo aver testato un avanzamento corretto senza errori del server master.

Nota: dopo un avanzamento, in determinate circostanze potrebbe essere opportuno scambiare i ruoli dei server master e di replica senza sovrascrivere i dati del server master originario con i dati del server di replica. A tale scopo, utilizzare l'opzione **Ripristino server attivo** (a pagina 265).

Avvio della regressione

Per avviare una regressione, procedere come segue:

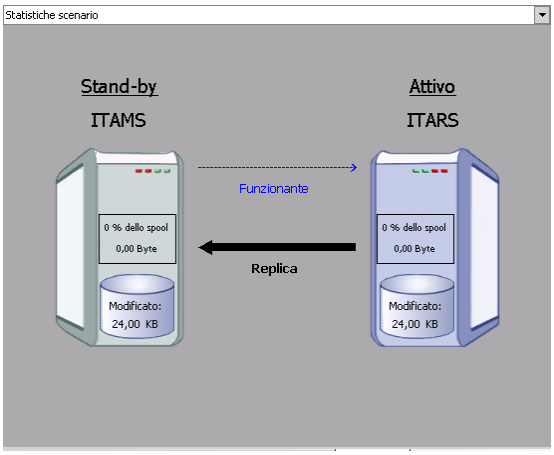
1. Assicurarsi che i server master e di replica siano disponibili in rete e che il modulo sia in esecuzione.
2. Aprire la Gestione e selezionare lo scenario desiderato dal riquadro Scenario.
3. Ignorare questo passaggio se lo scenario precedente è già in esecuzione e andare al passaggio 7.

   Se lo scenario precedente non è in esecuzione, selezionare il pulsante **Esegui** per avviare lo scenario. Arcserve RHA rileva che si è verificato un avanzamento, ne verifica lo stato e la configurazione e richiede di approvare l'esecuzione dello scenario precedente.

   Nota: il pulsante **Avanzate** consente di aprire un ulteriore riquadro con informazioni dettagliate sugli host che partecipano allo scenario.
4. Fare clic sul pulsante **Esegui** per avviare lo scenario precedente.

   Viene visualizzata la finestra di dialogo **Esegui.**
5. Per Microsoft Exchange, selezionare **Sincronizzazione a blocchi.** Per file server, fare clic su Sincronizzazione file quindi su **OK**. Viene avviata la risincronizzazione.

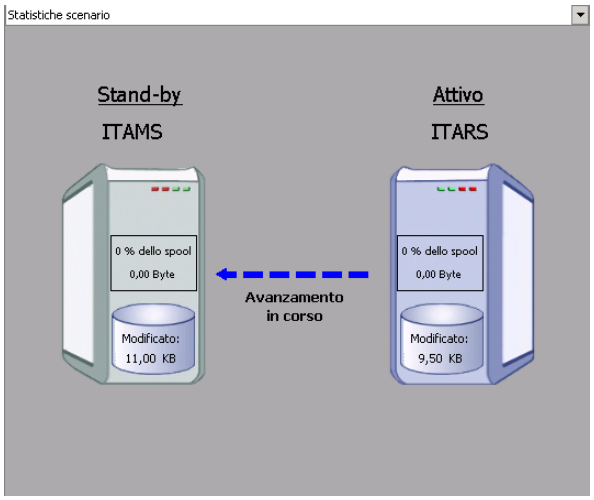
   Attendere sino al completamento della risincronizzazione.
6. Quando la sincronizzazione sarà completata, si riceverà il seguente messaggio nel riquadro Eventi: **Tutte le modifiche avvenute durante il periodo di sincronizzazione sono state replicate**. A questo punto, verrà avviata la replica dal server attivo al server in stand-by.



7. È ora possibile invertire i ruoli tra i server master e di replica. Per invertire i ruoli quando lo scenario precedente è in esecuzione, fare clic sul pulsante **Esegui avanzamento** oppure selezionare l'opzione **Esegui avanzamento** dal menu **Strumenti.**

   Verrà visualizzato un messaggio di conferma.

8. Fare clic su **Sì** nella finestra di conferma **Esegui avanzamento**. Questa procedura consente di avviare una regressione dal server di replica originario al server master.



9. Al termine della regressione, i ruoli dei server verranno nuovamente invertiti e lo scenario interrotto automaticamente.

È ora possibile eseguire nuovamente lo scenario nello stato originario (successivo).

Recupero del server attivo

In determinate circostanze, potrebbe essere necessario impostare in maniera intenzionale come attivo il server master o di replica, senza completare il processo di sincronizzazione. Ciò può verificarsi quando, ad esempio, è stato eseguito un avanzamento ma i dati sul server di replica non sono stati modificati, mentre sul server master potrebbero esserci dati anche più recenti. In questo caso, è possibile rendere non necessaria la sincronizzazione dei dati dal server di replica al server master. Con Arcserve RHA è possibile selezionare manualmente l'opzione del server attivo mediante un processo denominato **Ripristina server attivo**.

Potrebbero verificarsi casi in cui il processo di avanzamento non è stato completato correttamente e l'utilizzo dell'opzione **Ripristina server attivo** non risolve il problema, oppure potrebbe essere che non si desideri utilizzare questa opzione. In tal caso, è possibile ripristinare manualmente il server attivo al di fuori della Gestione. Il tipo di procedura da utilizzare dipende dal tipo di metodo di reindirizzamento utilizzato per l'avanzamento.

Le opzioni disponibili per il ripristino del server attivo a seguito di un mancato completamento dell'avanzamento sono le seguenti:

- Utilizzo dell'opzione Ripristina server attivo dalla Gestione (a pagina 265).
- Ripristino manuale del server attivo al di fuori della Gestione (a pagina 267).

Ripristino del server attivo mediante la Gestione

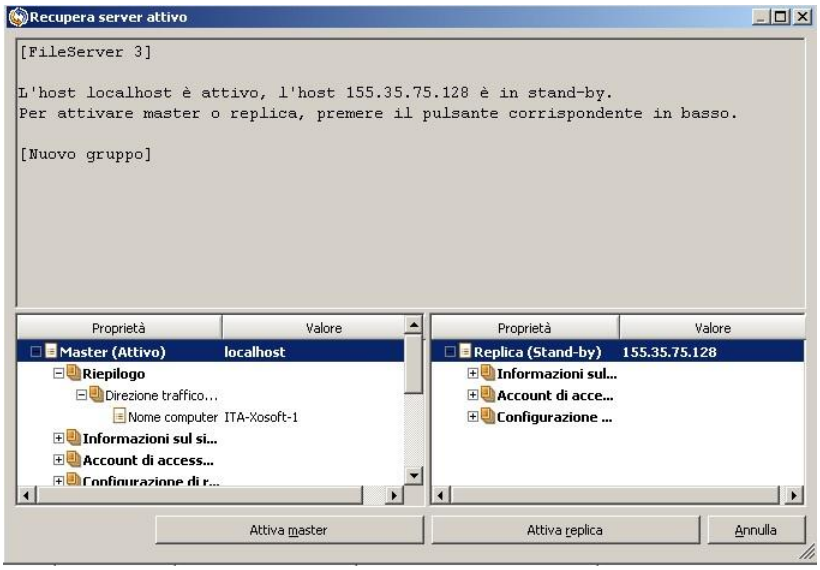
Se il processo di avanzamento non viene completato correttamente, Arcserve RHA consente di selezionare manualmente il server che dovrà fungere da server attivo durante un processo denominato **Ripristina server attivo**.

Importante: sebbene questa opzione sia l'ideale in determinate situazioni, si consiglia di utilizzarla con cautela. Se usata in maniera impropria, potrebbe verificarsi una perdita di dati. In genere, Arcserve RHA non consente l'esecuzione dell'avanzamento da un host all'altro fino al completamento della sincronizzazione di tutti i dati. È progettato in questo modo per evitare che gli utenti vengano reindirizzati a un set di dati non aggiornati e quindi per evitare la sovrascrittura di un set di dati più aggiornato. Quando si utilizza l'opzione **Ripristina server attivo**, Arcserve RHA reindirizza gli utenti su uno dei server, a prescindere dal server che dispone dei dati corretti. Pertanto, come amministratore, occorre verificare manualmente che il server che si sta rendendo attivo sia quello con il set di dati più recente.

Per ripristinare il server attivo mediante la Gestione:

1. Dal riquadro Scenario, selezionare lo scenario del quale si desidera recuperare il server e arrestarlo.
2. Dal menu **Strumenti**, scegliere l'opzione **Ripristina server attivo**.

   Arcserve RHA individua l'host attivo e presenta i risultati nella finestra di dialogo **Ripristina server attivo**.



3. Fare clic sul pulsante di **attivazione del master** oppure su quello di **attivazione della replica**, a seconda del server che si desidera rendere attivo.

   Nel riquadro eventi vengono visualizzati messaggi che informano l'utente che uno dei server è diventato attivo mentre l'altro è diventato inattivo. A questo punto, l'host selezionato diventa il server attivo e gli utenti vi saranno reindirizzati.

Importante: se si verifica un avanzamento standard in una situazione di emergenza e gli utenti vengono reindirizzati al server di replica per un certo periodo di tempo, è importante replicare sul server master tutte le modifiche apportate sul server di replica, prima di renderlo attivo. In tale situazione, l'opzione**Ripristina server attivo** potrebbe causare una perdita di dati.

Ripristino del server attivo senza utilizzare Gestione

Se il processo di avanzamento non viene completato correttamente per qualsivoglia ragione, e l'utilizzo dell'opzione **Ripristina server attivo** dalla Gestione non risolve il problema, è possibile eseguire una delle seguenti attività manuali a seconda del metodo di reindirizzamento utilizzato:

- Se viene utilizzato il metodo di reindirizzamento con **IP di spostamento,** rimuovere manualmente l'IP supplementare dal master (a pagina 267).
- Se viene utilizzato il metodo di reindirizzamento **Cambia nome computer**, scambiare manualmente i nomi computer del master e della replica (a pagina 268).
- Se vengono utilizzati entrambi i metodi di reindirizzamento **IP di spostamento** e **Cambia nome computer,** rimuovere manualmente l'IP supplementare dal master, e scambiare manualmente i nomi computer del master e della replica (a pagina 269).

Recupero manuale di un server non funzionante con il metodo Indirizzo IP di spostamento

Per recuperare un server non funzionante quando è in uso il metodo Indirizzo IP di spostamento, procedere come segue:

1. Avviare il server master senza connessione di rete per evitare conflitti di indirizzo IP.

   La verifica Funzionante dal master alla replica, riconosce eventuali errori presenti nella risorsa e sceglie la replica originale come server attivo.

2. Dalla finestra di dialogo **Impostazioni avanzate TCP/IP** sul master, rimuovere l'indirizzo IP supplementare.
3. Riavviare il server master e ristabilire la connessione alla rete.
4. Se lo scenario HA non è già in esecuzione, avviarlo dalla Gestione facendo clic sul pulsante **Esegui**.

   Se la proprietà **Esegui lo scenario di replica inversa dopo l'avanzamento** è impostata su Attivo, lo scenario viene eseguito all'indietro, dalla replica originale al master originale. Il master originale fungerà, quindi, da server in stand-by.

5. Attendere il completamento della sincronizzazione.
6. Per restituire il ruolo attivo al server master, eseguire un avanzamento manuale facendo clic sul pulsante **Esegui avanzamento** sulla barra degli strumenti standard.

   Nota: si consiglia di eseguire l'avanzamento manuale al di fuori degli orari di lavoro.

Recupero manuale di un server con errori utilizzando il metodo Cambia nome computer

Per eseguire il recupero manuale di un server con errori utilizzando il metodo di reindirizzamento Cambia nome computer, procedere come segue:

1. Avviare il server master senza connessione di rete, in modo da evitare duplicati nei nomi delle reti.

   La verifica Funzionante dal master alla replica, riconosce eventuali errori presenti nella risorsa e sceglie la replica originale come server attivo.

2. Rinominare il server master <NuovoNomeServer>-RHA e spostarlo in un gruppo di lavoro temporaneo.

   Ad esempio, se il nome del server è "Server1", rinominarlo in "Server1-RHA".

3. Sarà necessario riavviare il computer.

   Dopo il riavvio, verrà visualizzato un errore indicante che **almeno uno dei servizi non è stato avviato**. Ignorare questo messaggio, del tutto normale in tali circostanze, in quanto il modulo viene eseguito generalmente in un account di dominio.

4. Effettuare un collegamento a una rete.

5. Aggiungere nuovamente il computer al dominio, assicurandosi di utilizzare il nome -RHA assegnato al punto 2.

6. Riavviare il computer.

7. Se lo scenario HA non è già in esecuzione, avviarlo dalla Gestione facendo clic sul pulsante **Esegui** nella barra degli strumenti standard.

   Se è stata selezionata la proprietà **Esegui lo scenario di replica inversa dopo l'avanzamento**, lo scenario viene eseguito all'indietro, dalla replica originale al master originale. Il master originale funge ora da server in stand-by.

8. Attendere il completamento della sincronizzazione.

9. Per restituire il ruolo attivo al server master, eseguire un avanzamento manuale facendo clic sul pulsante **Esegui avanzamento** sulla barra degli strumenti standard.

   Nota: si consiglia di eseguire l'avanzamento manuale al di fuori degli orari di lavoro.

Recupero manuale di un server con errori - IP di spostamento e Cambia nome computer

Per recuperare manualmente un server non funzionante quando sono in uso i metodi di reindirizzamento IP e Cambia nome computer, procedere come segue:

1. Risolvere eventuali problemi hardware che possono aver causato l'avanzamento.
2. Riavviare il server senza connessione di rete per evitare conflitti di indirizzi IP.

   La verifica Funzionante dal master alla replica, riconosce eventuali errori presenti nella risorsa e sceglie la replica originale come server attivo.
3. Dalla finestra di dialogo **Impostazioni avanzate TCP/IP** sul master, rimuovere l'indirizzo IP supplementare.
4. Dalla finestra di dialogo **Proprietà del sistema**, nella scheda **Nome computer**, modificare il nome computer in <NomeServer>-RHA. Ad esempio, se il nome del server è Server 3, rinominarlo Server 3-RHA.
5. Assegnare il server a un gruppo di lavoro temporaneo.
6. Riavviare il computer per rendere effettive le modifiche. Dopo il riavvio, connettersi nuovamente alla rete. Verrà visualizzato un messaggio di errore indicante che **almeno uno dei servizi ha riportato errori durante l'avvio del sistema.** Ignorare questo messaggio, del tutto normale in tali circostanze, in quanto il modulo viene eseguito generalmente in un account di dominio.
7. Aggiungere nuovamente il server al dominio, assicurandosi di utilizzare il nome -RHA e riavviare.
8. Se lo scenario HA non è già in esecuzione, avviarlo dalla Gestione facendo clic sul pulsante **Esegui** nella barra degli strumenti standard. Se è stata selezionata l'opzione **Esegui lo scenario di replica inversa dopo l'avanzamento**, lo scenario viene eseguito all'indietro, dalla replica originale al master originale. Il master originale funge ora da server in stand-by.
9. Attendere il completamento della sincronizzazione.
10. Per restituire il ruolo attivo al server master, eseguire un avanzamento manuale facendo clic sul pulsante **Esegui avanzamento** sulla barra degli strumenti standard.

    Nota: si consiglia di eseguire l'avanzamento manuale al di fuori degli orari di lavoro.

Nozioni fondamentali sul sistema High Availability e sulle procedure di avanzamento e regressione

Uno scenario High Availability integra tutte le funzionalità e il flusso di lavoro di uno scenario di replica, ma in più presenta tre nuovi elementi importanti: verifica preliminare all'esecuzione, monitoraggio del server master e dell'applicazione in esecuzione su tale server e processo di avanzamento.

- **Verifica preliminare all'esecuzione**

  Durante un avanzamento, molte cose possono andare per il verso sbagliato: potrebbero verificarsi problemi con le autorizzazioni oppure con la configurazione dell'applicazione o ancora con le impostazioni dello stesso scenario HA. Per questo motivo, quando viene creato e avviato uno scenario HA, Arcserve RHA esegue un'approfondita serie di controlli. Tali controlli sono mirati a determinare se è possibile rilevare le questioni comuni che notoriamente causano problemi durante l'avanzamento. Quando i problemi vengono rilevati durante la verifica preliminare all'esecuzione, verranno visualizzati errori e avvisi che richiedono di risolverli prima di eseguire lo scenario HA.

- **Monitoraggio automatico del server master e dell'applicazione in esecuzione su di esso**

  Non appena viene avviato lo scenario, il server di replica controlla il server master su base pianificata, per impostazione predefinita ogni 30 secondi. Esistono tre tipi di controlli di monitoraggio: una richiesta ping inviata al server master per verificare che sia attivo e risponda; un controllo del database che consente di verificare che i servizi appropriati siano in esecuzione e i dati siano in buono stato; un controllo definito dall'utente, personalizzabile dall'utente per il monitoraggio di applicazioni specifiche.

  Se si verifica un errore in qualsiasi parte del set, l'intero controllo viene considerato come non riuscito. Se tutti i controlli non riescono in un periodo di timeout configurato (per impostazione predefinita, 5 minuti), il server master verrà considerato come inattivo. A seconda della configurazione dello scenario HA, Arcserve RHA invia un avviso all'utente oppure avvia automaticamente un avanzamento.

- **Flusso di lavoro di avanzamento e regressione**

  In uno scenario HA iniziale, il server master è il computer attivo e il server di replica è il computer in stand-by. Il computer in stand-by controlla continuamente lo stato del computer attivo, al fine di determinare se è funzionante e per stabilire se assumere il ruolo attivo.

  È possibile attivare un avanzamento automaticamente oppure premendo semplicemente un pulsante. La prima volta che si esegue un avanzamento, il server di replica che era in stand-by diventa il computer attivo, e il server master torna in modalità stand-by (supponendo che sia ancora operativo). Quando il server master (ora server in "stand-by") è pronto, è possibile avviare il processo di regressione, in modo automatico o manuale. In seguito alla regressione, il server master ridiventa attivo e il server di replica torna alla precedente modalità di stand-by e al ruolo di monitoraggio.

  Nota: in seguito a una perdita di connessione, durante il tentativo di riconnessione, un nodo (master o di replica) tenta di determinare il proprio ruolo. Se entrambi i nodi si riconoscono come master, quando viene ristabilita la connessione l'ultimo nodo master attivo continuerà ad avere ruolo di master, mentre l'altro assumerà il ruolo di nodo di replica in stand-by.

Importante: Dopo l'avanzamento, il servizio "server" sul server in stand-by, utilizzato per il supporto di file, la stampa e la condivisione di named pipe, diventa inaccessibile per i dieci minuti successivi all'avanzamento (cfr. l'opzione HASharesAccessTimeout nel file ws_rep.cfg).

Impostazione delle proprietà High Availability

In questo capitolo vengono descritte le modalità di configurazione delle proprietà High Availability e viene fornito l'elenco delle proprietà HA, i valori corrispondenti e una spiegazione per ciascuna proprietà.

Nota: queste opzioni sono disponibili solo per coloro in possesso di una licenza per High Availability.

Alcune proprietà sono applicabili solo a determinati tipi di server (ad esempio, Exchange, SQL, ecc.). Per ulteriori informazioni, consultare la Guida operativa specifica.

Argomenti correlati:

- Configurazione delle proprietà High Availability (a pagina 272)
- Host attivi e in stand-by (a pagina 285)
- Reindirizzamento con IP di spostamento (a pagina 285)

Configurazione delle proprietà High Availability

I valori delle proprietà HA determinano il comportamento predefinito dell'intero scenario per quanto riguarda il metodo di reindirizzamento, la gestione dei database e molto altro.

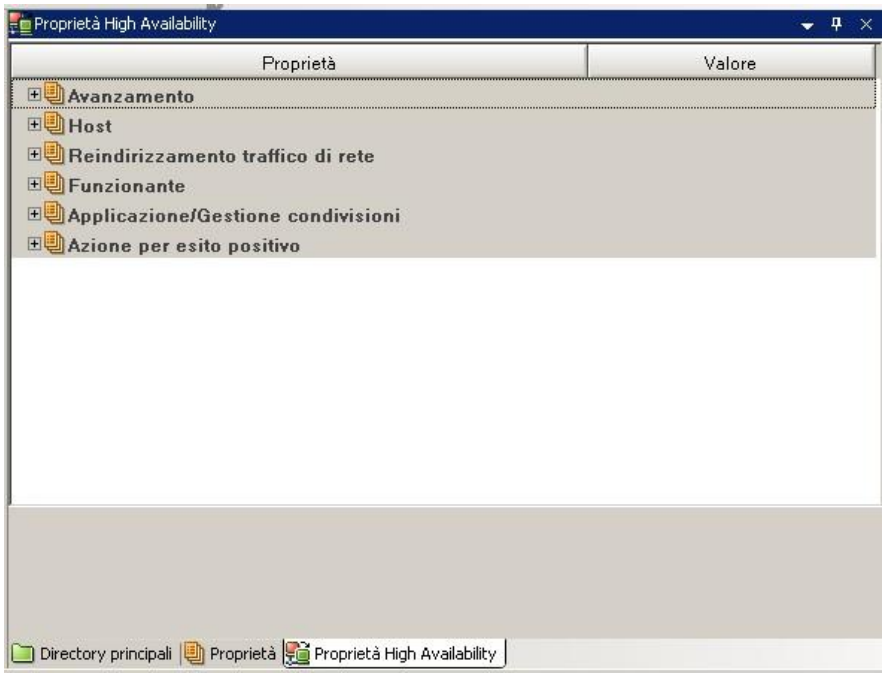
Note:

- Il riquadro Proprietà e le relative schede (Directory principali, Proprietà, Statistiche) sono sensibili al contesto. Il contenuto visualizzato viene modificato quando viene selezionato un nodo diverso dalla cartella dello scenario.
- Per configurare le proprietà di uno scenario, è necessario interrompere lo scenario.

Per impostare le proprietà dello scenario, procedere come segue:

1. Dal riquadro Scenario, selezionare lo scenario HA del quale si desidera configurare le proprietà.
2. Nel riquadro Struttura a sinistra, selezionare la scheda Proprietà High Availability.

   Viene visualizzato un elenco delle Proprietà High Availability.



Nota: uno scenario in esecuzione ha lo sfondo di colore grigio, mentre gli scenari non in esecuzione hanno uno sfondo di colore bianco.

3. Se lo scenario è in esecuzione, fare clic sul pulsante **Interrompi** sulla barra degli strumenti. Lo scenario viene interrotto.
4. Nell'elenco Proprietà scenario, aprire il gruppo desiderato, selezionare la proprietà richiesta e selezionare o immettere i valori appropriati. È possibile immettere manualmente alcuni valori nel campo di una casella di modifica mentre è possibile selezionarne altri da una casella combinata facendo clic sul valore predefinito.
5. Dopo aver impostato le proprietà richieste, fare clic sul pulsante **Salva** nella barra degli strumenti standard per salvare e applicare le proprie modifiche.

Nozioni fondamentali sulle proprietà High Availability

In questa sezione vengono elencate le proprietà High Availability, i valori corrispondenti, e viene fornita una spiegazione per ciascuna proprietà. Vengono inoltre illustrati i concetti di host attivo e in stand-by. Le proprietà High Availability vengono classificate in base alla loro posizione nel rispettivo gruppo di proprietà:

- Avanzamento (a pagina 274)
- Host (a pagina 274)
- Reindirizzamento del traffico di rete (a pagina 275)
- Funzionante (a pagina 281)
- Gestione database/Applicazione/Gestione condivisioni (a pagina 283)
- Azione in caso di esito positivo (a pagina 284)

Avanzamento

Il sistema controlla continuamente la presenza di una situazione di avanzamento, come definito nelle proprietà Funzionante (a pagina 281) e informa l'utente in base alle impostazioni di notifica definite. Quando il sistema rileva una situazione di avanzamento, l'opzione **Esegui automaticamente l'avanzamento** viene selezionata in modo da determinare se occorre eseguire un avanzamento automatico oppure inviare solo una notifica della situazione. Nel secondo caso, è possibile attivare l'avanzamento mediante il comando di menu o il pulsante della barra degli strumenti **Esegui avanzamento**.

Nome host di avanzamento

Immettere il nome e l'indirizzo IP dell'host in cui è installato l'agente. È possibile scegliere solo uno server di replica.

Ogni volta che si modifica il nome/IP o il nome/IP del server master, tutte le proprietà di avanzamento verranno reimpostate sui relativi valori predefiniti.

Esegui automaticamente l'avanzamento

Quando quest'opzione è attivata, l'avanzamento viene avviato automaticamente se il server master è inattivo o se viene rilevato un errore del database.

Esegui lo scenario di replica inversa dopo l'avanzamento

Dopo un avanzamento, questa opzione determina se la replica in direzione inversa deve iniziare automaticamente.

Se viene attivata l'opzione, Arcserve RHA verifica che venga conservata l'integrità dei dati. Se i dati sono rilevati come coerenti, verrà evitata la risincronizzazione e verrà avviato lo scenario di ritorno. Tuttavia, negli scenari DB in cui questa opzione è attivata, la replica inversa viene avviato in stato di sospensione. La replica verrà ripresa solo dopo che il database sul server attivo avrà superato tutti i test in genere eseguiti nelle proprietà **Controlla DB** e nelle proprietà **Funzionante**.

Host

Nome master completo

Indica il nome completo dell'host master. Il nome viene ottenuto automaticamente dal sistema operativo e non è possibile modificarlo manualmente.

Nome completo di replica

Indica il nome completo dell'host replica. Il nome viene ottenuto automaticamente dal sistema operativo e non è possibile modificarlo manualmente.

Reindirizzamento del traffico di rete

Esistono tre metodi di reindirizzamento:

- IP di spostamento
- Reindirizza DNS
- Cambia nome computer
- Cambia alias computer

È inoltre possibile specificare script definiti dall'utente per ciascun tipo di server.

I tre metodi di reindirizzamento possono essere utilizzati in base alla tabella seguente:

	IP di spostamento	**Reindirizza DNS**	**Cambia nome computer**	**Cambia nome alias**
Microsoft Dynamics	No	Sì	Sì	Sì
File server	Sì	Sì	Sì	Sì
HA per sistemi completi	No	Sì	No	No
Exchange	Sì	Sì	No	Sì
Oracle	Sì	Sì	No	Sì
SQL	Sì	Sì	Sì	Sì
IIS	Sì	Sì	Sì	Sì
Servizio di controllo	No	Sì	Sì	Sì
SharePoint	Sì	Sì	Sì	Sì
VMware vCenter	Sì	Sì	Sì	Sì
Hyper-V	No	Sì	No	No

Nota: per nomi alias di computer, Arcserve RHA supporta l'accesso UNC.

In seguito a un avanzamento, gli A-record dei server master e replica vengono modificati sul server DNS, a seconda dei metodi di reindirizzamento di rete selezionati. La tabella seguente mostra i metodi di reindirizzamento di rete che interessano l'A-record DNS.

- Se il metodo di reindirizzamento di rete è IP di spostamento, l'A-record DNS non viene coinvolto.
- Se il metodo di reindirizzamento di rete è Reindirizza DNS, il master dell'A-record rimanda all'IP di replica dopo l'avanzamento, mentre l'A-record replica non viene modificato.
- Se il metodo di reindirizzamento di rete è Cambia nome computer, l'A-record master viene modificato in Master-RHA dopo l'avanzamento e l'A-record replica viene modificato in master.
- Se i metodi di reindirizzamento di rete sono Reindirizza DNS e Cambia nome computer, il risultato è uguale a quello del metodo Reindirizza DNS.

Se si desidera mantenere l'A-Record replica, utilizzare il metodo di reindirizzamento Reindirizza DNS oppure i metodi DNS e Cambia nome computer.

IP di spostamento

Durante l'avanzamento, gli IP di avanzamento vengono rilasciati sull'host attivo e aggiunti all'host in stand-by. Questo metodo di reindirizzamento è applicabile solo quando sia il server master sia il server di replica si trovano sulla stessa subnet di IP.

L'attivazione o la disattivazione influiscono sulle opzioni disponibili nella proprietà Controlla con per Invia richiesta ping. Fare riferimento all'argomento Funzionante (a pagina 281).

Aggiungi IP/Maschera

Immettere gli indirizzi IP per il computer attivo che verranno trasferiti al computer in stand-by durante l'avanzamento. L'indirizzo IP del server master definito nelle relative proprietà deve essere diverso dagli indirizzi IP immessi qui.

Per aggiungere l'IP/Maschera, procedere come segue:

1. Fare clic sull'elemento della struttura: Fare clic qui per aggiungere un nuovo IP o una nuova maschera.

   Viene visualizzata la finestra di dialogo Indirizzo IP.

2. Immettere i dati di IP/Maschera appropriati nella finestra di dialogo, quindi fare clic su OK.

   Viene aggiunta una nuova voce all'elenco, quindi aperta una nuova riga per un'altro IP/Maschera. Immettere tutte le voci desiderate.

Note:

- L'indirizzo IP del server master nella scheda Proprietà sotto Connessione host (l'IP del server master immesso nella creazione guidata dello scenario) NON deve essere uno degli indirizzi IP inclusi in questo elenco.
- Se la proprietà IP di spostamento o Reindirizza DNS è attivata, Arcserve RHA disattiva la registrazione DNS dinamica per il server master. (la casella di controllo Register this connection's address in DNS (Registra indirizzo di collegamento in DNS) nella finestra di dialogo Impostazioni avanzate TCP/IP è deselezionata).

Reindirizza DNS

Durante l'avanzamento, il record A del server master verrà aggiornato. Questa opzione di reindirizzamento è applicabile quando il server master e il server di replica si trovano su una diversa subnet di IP oppure sulla stessa subnet.

Se la proprietà IP di spostamento o Reindirizza DNS è attivata, Arcserve RHA disattiva la registrazione DNS dinamica per il server master. (la casella di controllo Register this connection's address in DNS (Registra indirizzo di collegamento in DNS) nella finestra di dialogo Impostazioni avanzate TCP/IP è deselezionata).

Indirizzi IP dei server DNS

Immettere gli indirizzi IP dei server DNS da aggiornare. Arcserve RHA esegue il tentativo di aggiornare tutti i server elencati. Tuttavia, l'avanzamento viene considerato riuscito anche se è stato eseguito correttamente un solo aggiornamento.

Per immettere il valore, fare clic sulla voce: Fare clic qui per aggiungere un nuovo indirizzo IP.

Durata DNS

Immettere il numero di secondi per i server Time-To-Live DNS. Questo valore verrà modificato nel server DNS per il record A che è stato aggiornato.

Integrazione di Active Directory

Specificare se sul server DNS è integrato Active Directory. Se il DNS del server master si trova su una piattaforma Windows ed è integrato con Active Directory, impostare questa opzione su Attivato.

Nome file del codice DNS (percorso completo)

Specificare il percorso completo del file contenente la chiave protetta DNS. Questo campo viene visualizzato solo quando AD integrato è disattivato.

Indirizzi IP del server master/di replica nel DNS

Specificare gli indirizzi IP del server master/di replica nel relativo server DNS.

Il record DNS del server master viene aggiornato durante ogni avanzamento: nell'avanzamento dal server master al server di replica, gli indirizzi nel record DNS del server master verranno sostituiti dagli indirizzi del server di replica. Nella regressione dal server di replica al server master, verranno ripristinati i valori originali degli indirizzi.

Per immettere il valore, fare clic sulla voce: Fare clic qui per aggiungere un nuovo indirizzo IP.

Cambia nome computer

Questa opzione di reindirizzamento è applicabile durante l'utilizzo della risoluzione dei nomi NetBIOS per le connessioni con il master. Se il nome host e il nome NetBIOS non sono identici, non sarà possibile utilizzare questa opzione.

Durante l'avanzamento, il computer del server di replica verrà rinominato con il nome del computer master, mentre a quest'ultimo verrà assegnato un nome temporaneo (se il server master è funzionante). Durante la regressione, i nomi verranno ripristinati. Sia il nome host sia il nome NetBIOS verranno modificati. Se il reindirizzamento Cambia nome computer è abilitato nell'ambiente Active Directory, i server master e di replica devono essere membri dello stesso dominio o di un dominio attendibile.

Importante. Se si esegue il reindirizzamento di condivisioni file, in cui i client si connettono tramite il nome del server master, è necessario che Cambia nome computer sia abilitato. Ad esempio, se il nome del server master è fs01 e i client si connettono a \\fs01\sharename o \\fs01.domain.com\sharename, sarà necessario utilizzare il metodo Cambia nome computer. Si consiglia inoltre di abilitare un altro metodo. Il metodo più comune consiste nell'utilizzare sia il reindirizzamento DNS sia Cambia nome computer.

Quando si utilizza il metodo di reindirizzamento Cambia nome computer su sistemi Windows 2008 e sistemi Windows 2008 R2, è necessario riavviare il sistema in seguito a operazioni di avanzamento e regressione. È possibile eseguire uno scenario inverso solo dopo il riavvio del sistema, in quanto il nome computer diviene effettivo solo in seguito al riavvio. Si consiglia di attivare la proprietà Riavvia dopo un avanzamento e una regressione quando si utilizza questo metodo.

Nome computer master

Nome NetBIOS del computer master. Non è possibile modificare questo nome.

Nome computer di replica

Nome NetBIOS del computer di replica. Non è possibile modificare questo nome.

Riavvio dopo un avanzamento e una regressione

Dopo aver eseguito un avanzamento e una regressione, se questa opzione è attivata, i computer master e di replica verranno entrambi riavviati.

Utilizzo dell'alias nome computer

In seguito a un avanzamento, il nome computer della replica originale non verrà modificato. La replica utilizzerà invece il nome host master come alias, pertanto non sarà necessario riavviare il computer. Se l'opzione è attivata, è consigliabile attivare anche la proprietà Reindirizza DSN.

Script definiti dall'utente

Questa opzione consente di migliorare o sostituire i metodi di reindirizzamento standard mediante azioni richiamate tramite script definiti dall'utente.

Importante. Quando si utilizzano gli script, ognuno di essi deve risiedere nello stesso percorso e avere lo stesso nome sia sul server master sia sul server di replica.

Script di reindirizzamento da attivo a stand-by

- **Nome script:**

  Immettere il nome e il percorso completo dello script da eseguire sul computer attivo, se funzionante, allo scopo di reindirizzare i clienti al computer in stand-by oppure rilasciare le risorse di rete sull'host attivo.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Nota: anche lo **Script di reindirizzamento da Attivo a Stand-by** viene eseguito automaticamente all'avvio dello scenario HA. A questo punto, lo script viene eseguito sul server di replica in stand-by.

Script di reindirizzamento da Stand-by a Attivo.

- **Nome script:**

  Immettere il nome e il percorso completo dello script da eseguire sull'host in stand-by, allo scopo di reindirizzare i clienti su di esso o di aggiungere risorse di rete.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Identificare lo script di reindirizzamento traffico di rete

Richiesto per il supporto completo dei metodi di reindirizzamento personalizzati. Gli script personalizzati qui immessi vengono utilizzati per identificare il server attivo. Il modulo presuppone che:

- Se lo script era stato eseguito sull'host restituisce 0, l'host è attivo (tutte le relative risorse di rete o i suoi utenti vengono reindirizzati a questo host)
- Se lo script restituisce un valore diverso da zero, l'host è inattivo (oppure alcune delle risorse di rete sono assenti oppure gli utenti non vengono reindirizzati a questo host).

- **Nome script:**

  Specificare il nome e il percorso completo dello script da eseguire. Questo script determina se lo scenario successivo o precedente verrà eseguito all'avvio dello scenario. Lo script viene eseguito sia sul server master sia sul server di replica: quello tra i due che restituisce un valore pari a zero è il server attivo. Se entrambi restituiscono lo stesso valore, verrà segnalato un conflitto.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Cambia alias computer

Durante l'avanzamento, il nome alias viene rilasciato sull'host attivo e aggiunto all'host in stand-by.

Sono supportati i nomi alias NetBIOS e DNS CNAME. Per aggiungere nomi alias NetBIOS, creare un valore multistringa denominato OptionalNames con dati <aliasnames> nella chiave di registro seguente, quindi riavviare il servizio server.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters`

Nota: se il server master è un server del gruppo di lavoro, l'avanzamento mediante il nome dell'alias DNS non sarà supportato. Ciò si verifica quando l'utente del server del gruppo di lavoro non dispone dei privilegi di accesso alle informazioni DNS.

Nome alias

Immettere il nome alias dell'host attivo trasferito sull'host in stand-by durante l'avanzamento.

Aggiorna/Aggiungi/Elimina

Per impostazione predefinita, il nome alias viene configurato automaticamente al momento della creazione dello scenario High Availability. È possibile aggiungere o eliminare tutti gli alias oppure solo quelli selezionati.

Dopo la creazione dello scenario, è possibile aggiungere un nuovo alias nell'ambiente in uso. Per abilitare il nuovo alias, fare clic sul pulsante Aggiorna e caricare nuovamente le proprietà High Availability.

Funzionante

Arcserve RHA controlla continuamente che vi siano host attivi (in base al metodo *Invia richiesta ping*, *Connetti al database o Script definito dall'utente,* vedere di seguito). Questi controlli vengono effettuati a intervalli pianificati in funzione della frequenza di heartbeat.

Il controllo dello stato viene interpretato come segue:

- Se vi è un'indicazione che il computer attivo risponde, non verrà intrapresa nessuna nuova azione e il sistema continua a controllare a intervalli pianificati la frequenza di heartbeat.
- Se vi è un'indicazione che il computer attivo non risponde, questo verrà nuovamente controllato al successivo timeout di Heartbeat per un periodo massimo del timeout Funzionante. Se non vi è alcuna indicazione della risposta dell'host attivo entro il timeout Funzionante, Arcserve RHA esegue la notifica degli eventi. Simultaneamente, verifica se eseguire o no un avanzamento, come definito dalla proprietà Esegui automaticamente l'avanzamento.

Importante: Quando si utilizzano gli script, ognuno di essi deve risiedere nello stesso percorso e avere lo stesso nome sia sul server master sia sul server di replica.

Timeout per Funzionante (sec)

Se l'host in stand-by non riceve indicazione che l'host attivo è funzionante nel corso di questo intervallo (in secondi), verrà avviato l'avanzamento o la notifica. I controlli verranno eseguiti alla frequenza di hearbeat.

Il valore predefinito è 300 secondi.

Frequenza heartbeat (sec)

Intervallo (in secondi) per l'invio di richieste di heartbeat (che effettuano i seguenti controlli).

Il valore predefinito è 30 secondi.

Metodo di controllo

Invia richiesta ping

Le richieste ICMP vengono automaticamente inviate dall'host in stand-by all'host attivo, in modo da verificare che quest'ultimo risponda.

Le opzioni disponibili variano a seconda del valore impostato per la proprietà IP di spostamento. Per ulteriori informazioni, fare riferimento all'argomento Proprietà di reindirizzamento (a pagina 275).

- Se l'**IP di spostamento** è **Attivo**
- Durante l'avanzamento, l'indirizzo IP viene spostato dal computer attivo al computer in stand-by. Di conseguenza, il computer in stand-by deve verificare continuamente questo indirizzo IP.

  Nella proprietà **IP per ping**, immettere l'indirizzo IP sul quale eseguire il ping.

- Se l'**IP di spostamento** è **Non attivo**

  Durante l'avanzamento, l'indirizzo IP viene spostato dal computer attivo al computer in stand-by. Pertanto, definire due IP per il ping:

  IP per ping da master a replica
  Immettere l'indirizzo IP sul quale eseguire il ping. Quando il computer di replica è l'host attivo, verrà inviata una richiesta ICMP dal server master al server di replica. Se non si riceve una risposta entro due secondi, il computer di replica viene considerato non operativo.

  IP per ping da replica a master
  Immettere l'indirizzo IP al quale inviare il ping. Quando il computer master è l'host attivo, verrà inviata una richiesta ICMP dal server di replica al server master. Se non si riceve una risposta entro due secondi, il computer master viene considerato non operativo.

Connetti al database

[Solo per applicazioni di database] Quando la proprietà è attivata, Arcserve RHA effettua la connessione al database del computer attivo in base alla frequenza Heartbeat e verifica che i servizi di database siano in esecuzione e che tutti i database siano montati.

Script definiti dall'utente

Consentono di aumentare o sostituire i metodi di controllo standard con azioni definite dall'utente in script.

Verifica script sull'host attivo

Questo script viene eseguito sul server attivo per verificare se è in funzione.

- **Nome script:**

  Specificare il nome e il percorso completo dello script da eseguire. Arcserve RHA effettua la connessione al computer attivo a ogni timeout di Heartbeat ed esegue lo script. Se il valore restituito è pari a zero, il computer attivo risponde. Se il valore restituito è diverso da zero, il server attivo non risponde ed è richiesto l'avanzamento.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Verifica script sull'host in stand-by

Questo script viene eseguito sul server in stand-by per verificare che il server attivo sia funzionante.

- **Nome script:**

  Specificare il nome e il percorso completo dello script da eseguire. Arcserve RHA effettua la connessione al computer attivo a ogni timeout di Heartbeat ed esegue lo script. Se il valore restituito è pari a zero, il computer attivo risponde. Se il valore restituito è diverso da zero, il server attivo non risponde ed è richiesto l'avanzamento.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Gestione database/Applicazione/Gestione condivisioni

Automatico

Attivare questa opzione se si desidera che Arcserve RHA gestisca i servizi sul server database. Si verificano le condizioni descritte di seguito.

1. Durante la creazione dello scenario, l'elenco dei servizi applicazione (database) da gestire viene rilevato automaticamente.
2. Quando lo scenario è in esecuzione:
   - [DB]: i servizi DB sull'host attivo vengono avviati (se non sono già in esecuzione) e interrotti sull'host in stand-by (se sono in esecuzione).
3. Durante l'avanzamento:
   - [DB]: i servizi DB vengono interrotti sull'host attivo e avviati sul server in stand-by.

Script definiti dall'utente

Avvio del database/Avvio dello script di applicazione

Se la relativa opzione è attivata, viene eseguito uno script definito dall'utente per aumentare o sostituire l'avvio di servizi DB o l'avvio delle applicazioni. Questo si verifica durante l'esecuzione di uno scenario sull'host attivo oppure durante un avanzamento sull'host in stand-by.

Nome script (percorso completo)

Specificare il nome e il percorso completo dello script da eseguire.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Interruzione del database/Interruzione dello script di applicazione

Se la relativa opzione è attivata, viene eseguito uno script definito dall'utente per aumentare o sostituire l'interruzione di servizi DB o l'interruzione delle applicazioni. Questo si verifica durante l'esecuzione di uno scenario sull'host in stand-by o durante un avanzamento sull'host attivo.

- **Nome script (percorso completo)**

  Specificare il nome e il percorso completo dello script da eseguire.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti devono avere valori statici.

Azione in caso di esito positivo

Importante: Quando si utilizzano gli script, ognuno di essi deve risiedere nello stesso percorso e avere lo stesso nome sia sul server master sia sul server di replica.

Script definito dall'utente

Se impostato su Attivo, esegue uno script definito dall'utente. Le azioni richiamate dallo script verranno eseguite in seguito al corretto completamento di un avanzamento.

- **Nome script (percorso completo)**

  Specificare il nome e il percorso completo dello script. Questo script viene eseguito sul server attivo al termine dell'avanzamento.

- **Argomenti**

  Argomenti da trasmettere allo script specificato nella proprietà precedente. Gli argomenti hanno valori statici.

Host attivi e in stand-by

In uno scenario iniziale, il server master è il computer attivo e il server di replica è il computer in stand-by. Il computer in stand-by controlla continuamente lo stato di quello attivo, al fine di stabilire se assumere il ruolo attivo.

La prima volta che si esegue un avanzamento, il server di replica che era in stand-by diventa il computer attivo, e il server master torna in modalità stand-by (supponendo che sia ancora operativo). Quando il server master (ora server in "stand-by") è pronto, è possibile avviare il processo di regressione in cui il server master ridiventa attivo e il server di replica torna alla precedente modalità di stand-by e al ruolo di monitoraggio.

Reindirizzamento con IP di spostamento

In questa sezione viene illustrata la procedura necessaria per aggiungere il reindirizzamento dell'IP di spostamento nello scenario High Availability.

Importante: Utilizzare questo metodo solo quando entrambi i server si trovano sulla stessa subnet IP.

Aggiunta dell'indirizzo IP all'host master

Per utilizzare il metodo di reindirizzamento IP di spostamento negli scenari HA, è necessario aggiungere un indirizzo IP aggiuntivo all'host Master. (Questo indirizzo IP aggiuntivo viene indicato come **RHA-IP** nelle fasi seguenti). Il nuovo indirizzo IP verrà utilizzato per la comunicazione interna e la replica di Arcserve RHA. Questa operazione è necessaria poiché, quando si verifica l'avanzamento, l'IP originario del server master corrente non è più disponibile sul server master in quanto viene trasferito all'host di replica.

Per aggiungere l'indirizzo IP all'host master, procedere come segue:

1. Selezionare **Start**, **Impostazioni**, **Pannello di controllo**, **Connessioni di rete**, **Connessione alla rete locale (LAN)**.

   Viene visualizzata la finestra di dialogo **Stato di Connessione alla rete locale (LAN)**.

2. Nella scheda **Generale**, fare clic sul pulsante **Proprietà**.

   Viene visualizzata la finestra di dialogo **Proprietà - Connessione alla rete locale (LAN)**.

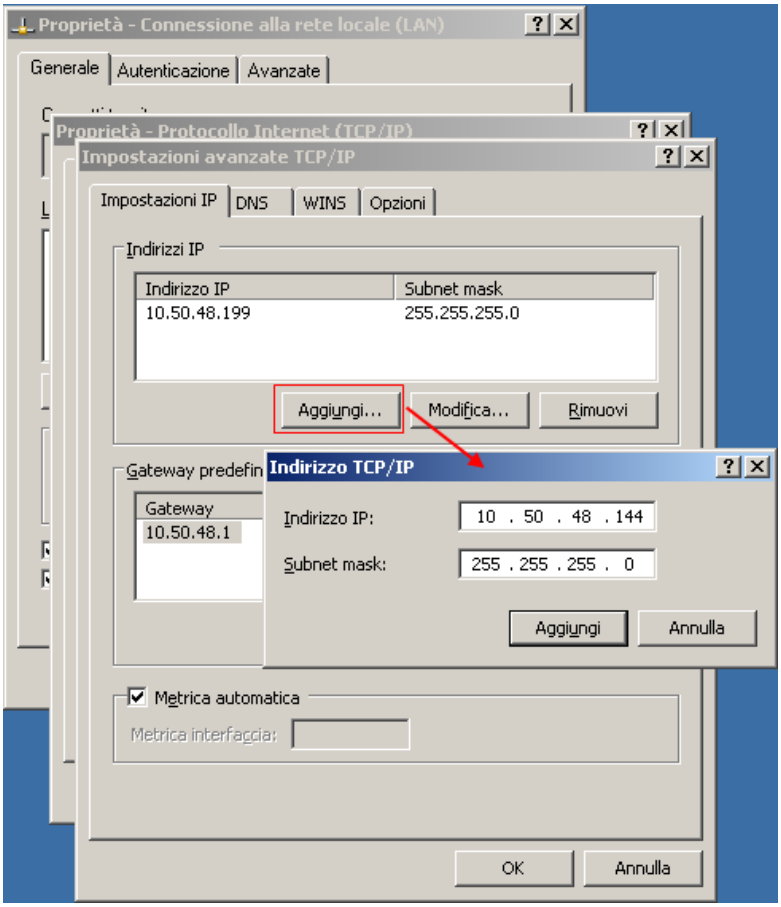
3. Nella scheda **Generale**, selezionare **Protocollo Internet (TCP/IP)**, quindi fare clic sul pulsante **Proprietà**.

   Viene visualizzata la finestra di dialogo **Proprietà Protocollo Internet (TCP/IP)**.

4. Nella scheda **Generale**, fare clic sul pulsante **Avanzate**.

   Viene visualizzata la finestra di dialogo **Impostazioni avanzate TCP/IP**.

5. Nella scheda **Impostazioni IP**, fare clic sul pulsante **Aggiungi**.
6. Viene visualizzata la finestra di dialogo **Indirizzo TCP/IP**.



7. Nella finestra di dialogo **Indirizzo TCP/IP**, immettere l'indirizzo IP aggiuntivo (IP RHA). Quindi, fare clic su Aggiungi.

   L'indirizzo IP aggiuntivo viene salvato e la finestra di dialogo **Indirizzo TCP/IP** si chiude.
8. Fare clic su **OK** su tutte le finestre di dialogo aperte, fino alla loro completa chiusura, e uscire dalle impostazioni di connessione alla rete locale.

Configurazione del metodo IP di spostamento mediante la Gestione

Dopo aver aggiunto l'indirizzo IP aggiuntivo all'host master, è necessario aggiungere l'indirizzo IP RHA agli scenari HA. È possibile aggiungere l'indirizzo IP RHA a uno scenario HA in due modi:

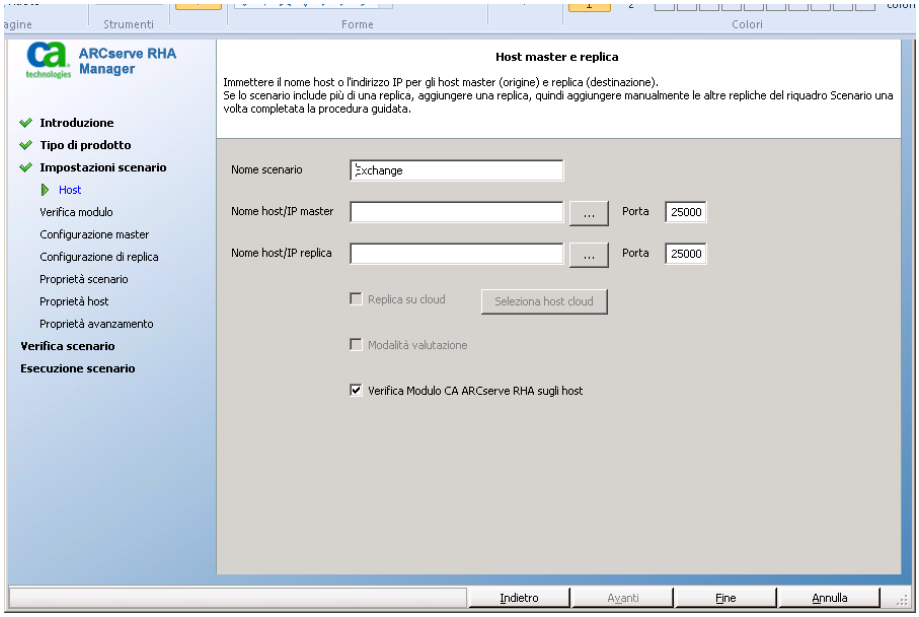
- Per i nuovi scenari, direttamente dalla Creazione guidata scenario.
- Per gli scenari esistenti, tramite modifica del nome host del server master.

Entrambe le procedure sono illustrate di seguito.

Aggiunta di un indirizzo IP RHA a nuovi scenari

Per aggiungere un indirizzo IP RHA a un nuovo scenario per il metodo di reindirizzamento IP di spostamento, procedere come segue:

1. Nella Creazione guidata scenario, nella schermata **Host master e replica**, immettere i dati descritti di seguito.
   - Nella casella **Nome host/IP master**, immettere l'indirizzo IP aggiuntivo (RHA-IP).
   - Nella casella **Nome host/IP di replica**, immettere l'indirizzo IP dell'host di replica, e non il nome host.



2. Fare clic su **Avanti** e procedere con la definizione dello scenario come di consueto fino alla visualizzazione della schermata **Proprietà avanzamento**.
3. Nella schermata **Proprietà avanzamento**, aprire il gruppo **Reindirizzamento traffico di rete**, selezionare la proprietà **IP di spostamento**, quindi impostare il valore su Attivo.

   Per impostazione predefinita, il secondo indirizzo IP dell'host master viene visualizzato nella casella **IP/Maschera**.

   Nota: se l'host master dispone di un solo indirizzo IP, la casella **IP/Maschera sarà vuota**.
4. Se sono presenti utenti finali che si collegano all'host master mediante il nome host, utilizzare i metodi **Reindirizza DNS** o **Cambia nome computer** unitamente al metodo **IP di spostamento**. Nel caso in cui non sia necessario utilizzare il nome host dell'host master, disabilitare l'opzione **Reindirizza DNS** impostando il relativo valore su Non attivo.
5. In seguito all'impostazione del metodo di reindirizzamento, fare clic su **Avanti** e procedere con la definizione dello scenario HA come di consueto.

Aggiunta di un indirizzo IP RHA a scenari esistenti

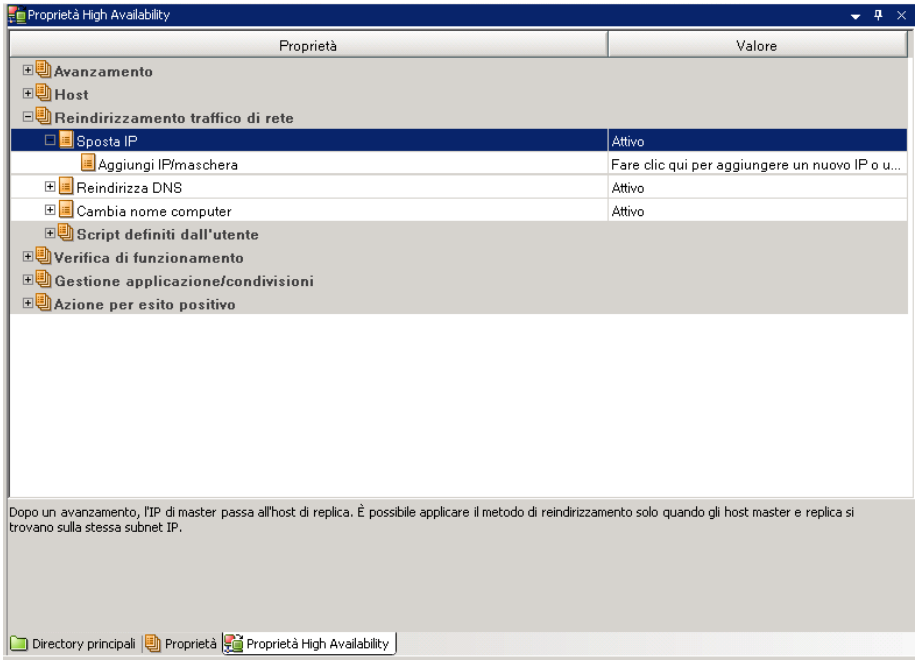
Prima di eseguire questa operazione, interrompere lo scenario.

Per aggiungere un indirizzo IP RHA a uno scenario esistente per il metodo di reindirizzamento IP di spostamento, procedere come segue:

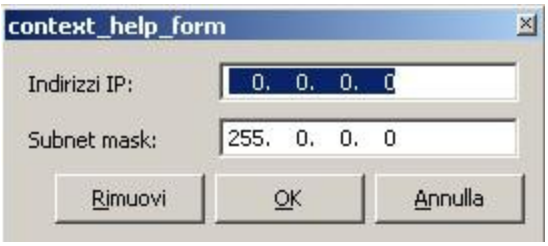
1. Nel riquadro Scenario, selezionare l'host master richiesto.
2. Fare clic con il pulsante destro del mouse sul server master e selezionare **Rinomina** dal menu di scelta rapida. Quindi, immettere l'indirizzo **IP RHA**.
3. Assicurarsi che l'host di replica sia definito mediante il relativo indirizzo IP e non mediante il nome host. Se necessario, immettere l'indirizzo IP dell'host di replica al posto del nome host.
4. Nel riquadro Struttura, selezionare la scheda **Proprietà High Availability**.

5. Aprire il gruppo **Reindirizzamento traffico di rete**, selezionare l'opzione **IP di spostamento**, quindi impostare il valore su Attivo.

   Viene visualizzata la proprietà **IP/Maschera**.

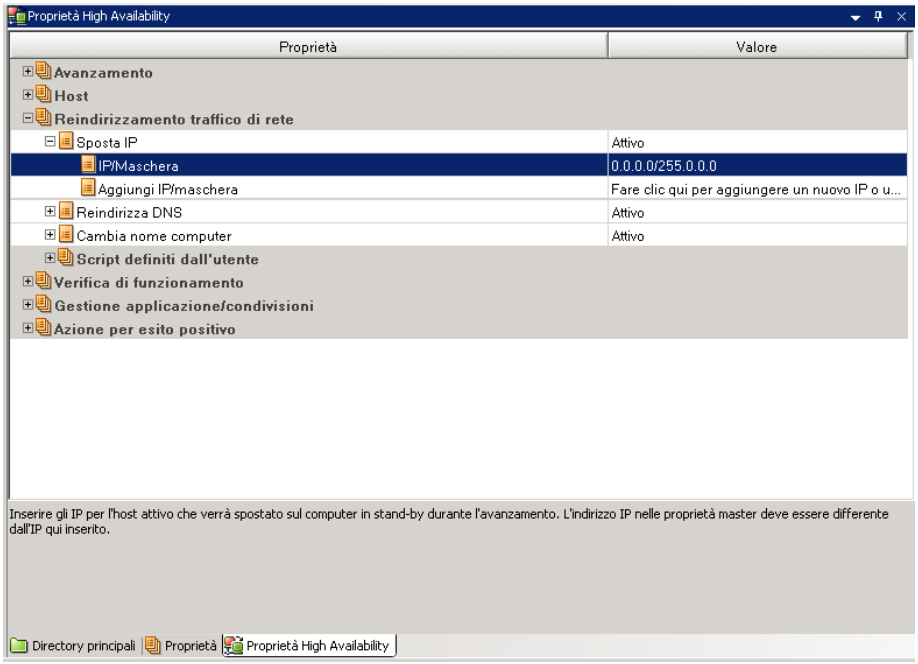


6. Fare clic sulla casella relativa al valore di **IP/Maschera**. Viene visualizzata la finestra di dialogo **Indirizzo IP**.



7. Immettere l'indirizzo IP originario dell'host master. Tale indirizzo IP verrà spostato sul computer in stand-by durante l'avanzamento. Fare quindi clic su **OK**.

   Nota: se si spostano più indirizzi IP, è possibile aggiungere più indirizzi IP di produzione selezionando **Fare clic qui per aggiungere un nuovo IP o una nuova maschera.**



8. Se sono presenti utenti finali che si collegano all'host master mediante il nome host, utilizzare i metodi **Reindirizza DNS** o **Cambia nome computer** unitamente al metodo **IP di spostamento**. Nel caso in cui non sia necessario utilizzare il nome host dell'host master, disabilitare l'opzione **Reindirizza DNS** impostando il relativo valore su Non attivo.

9. Per salvare le impostazioni, fare clic su **Salva** nella barra degli strumenti standard.

IP di spostamento del cluster

L'utilizzo del reindirizzamento dell'IP di spostamento con un server master cluster (MSCS con archiviazione condivisa) richiede l'aggiunta di un'ulteriore risorsa IP al gruppo di risorse del server Master. In questa sezione viene descritta la modalità di configurazione di questo metodo di reindirizzamento.

Nota: se entrambi i server Master e Replica sono cluster, eseguire le seguenti operazioni:

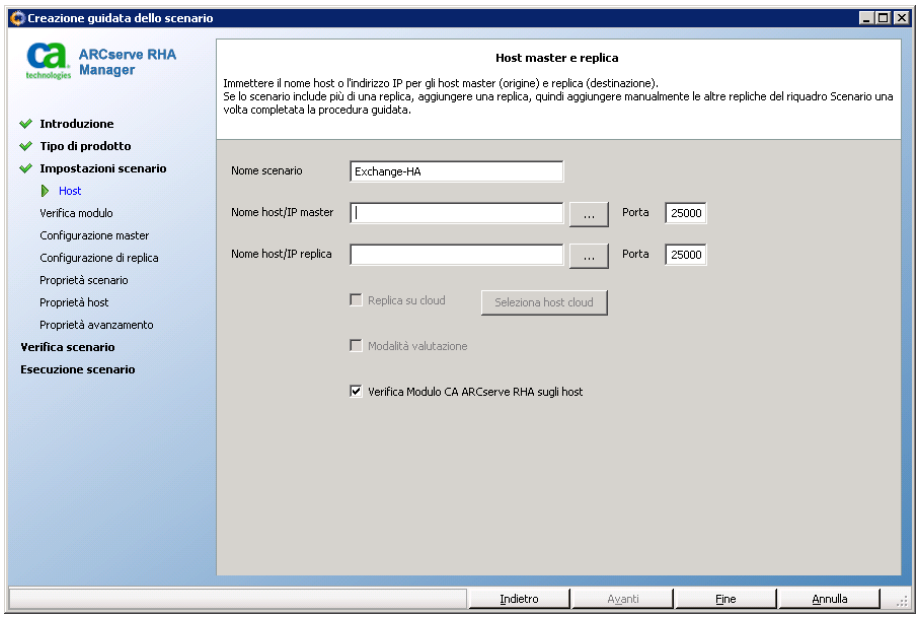
1. Creare manualmente una risorsa IP con l'indirizzo IP che si desidera spostare al cluster di replica, quindi disattivare la risorsa.
2. Creare uno scenario HA attenendosi alla procedura standard, quindi utilizzare il metodo di reindirizzamento Sposta IP. Verificare che la risorsa IP creata sul cluster di replica sia identica all'indirizzo IP che si desidera spostare.
3. Eseguire lo scenario normalmente.

Utilizzo della Gestione

In questa sezione viene illustrato nel dettaglio il reindirizzamento dell'IP di spostamento del cluster mediante la Gestione.

Nuovi scenari

Durante l'esecuzione iniziale della procedura guidata, immettere gli indirizzi IP RHA e del server di replica invece dei nomi dei server virtuale del cluster. Nella schermata seguente sono visualizzati l'indirizzo IP RHA immesso nel campo Nome host/IP master e l'indirizzo IP del server di replica immesso nel campo Nome host/IP di replica



Scenari esistenti

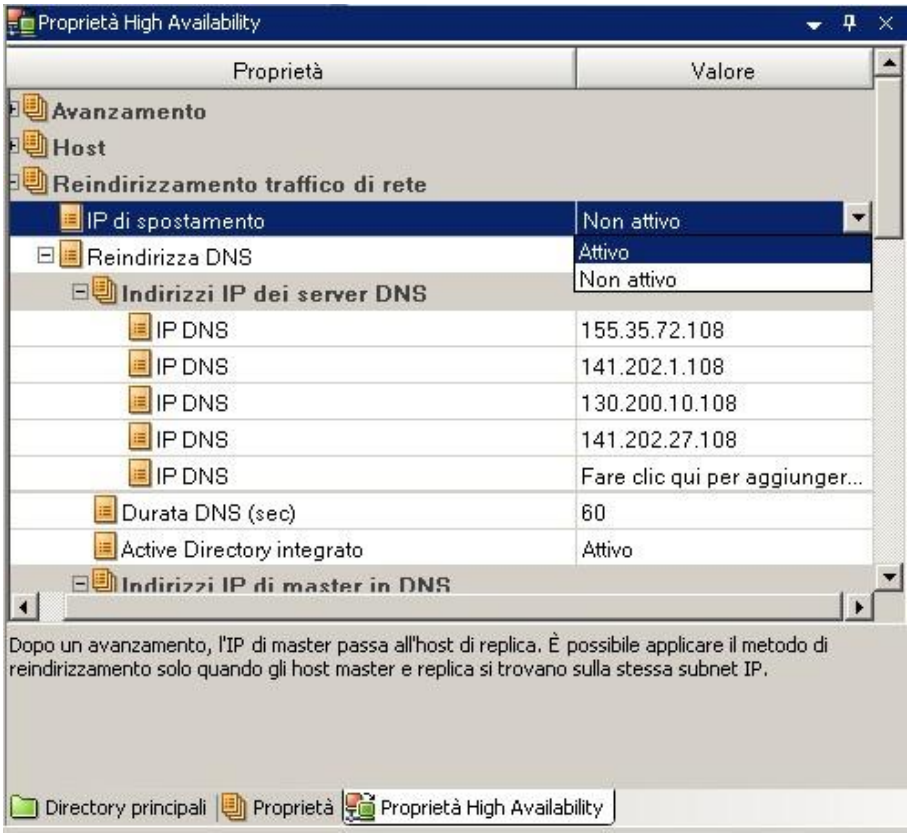
Per utilizzare l'IP di spostamento del cluster negli scenari esistenti, procedere come segue

1. Nel riquadro Scenario, selezionare l'host master richiesto.

2. Fare clic con il pulsante destro del mouse sul server master e selezionare **Rinomina** dal menu di scelta rapida. Quindi, immettere l'indirizzo IP RHA.

3. Nel riquadro Struttura, selezionare la scheda Proprietà High Availability e quindi selezionare il server di replica come host di avanzamento.

4. Impostare l'opzione **IP di spostamento** su Attivo. Assicurarsi che l'indirizzo IP sotto **IP di spostamento**, **IP/Maschera** corrisponda all'indirizzo IP del server di produzione, poiché questo sarà l'indirizzo IP di cui verrà eseguito l'avanzamento. Se si spostano più indirizzi IP, è possibile aggiungere vari indirizzi IP di produzione selezionando **Fare clic qui per aggiungere un nuovo IP o una nuova maschera**.



Utilizzo del cluster master

Per utilizzare l'IP di spostamento cluster tramite il cluster master, procedere come segue:

1. Aprire Amministrazione cluster.
2. Nel gruppo di risorse del cluster master, creare una nuova risorsa IP e denominarla **IP RHA**.
3. Mettere in linea questa risorsa e verificare che sia visibile dal server di replica tramite un comando ping. Il nuovo indirizzo IP verrà utilizzato per la comunicazione interna e la replica di Arcserve RHA. Ciò è necessario in quanto l'indirizzo IP di produzione corrente non è disponibile sul server master poiché dopo l'avanzamento è stato trasferito al server di replica.

Capitolo 11: Protezione del Servizio di controllo

In questa sezione vengono fornite istruzioni sulla replica dei dati del Servizio di controllo e sull'inversione dei ruoli di due servizi di controllo nei casi in cui il Servizio di controllo attivo non è disponibile. Inoltre, vengono dettagliatamente descritte le seguenti operazioni: creazione e utilizzo di uno scenario Servizio di controllo HA ed esecuzione di avanzamento e regressione del Servizio di controllo.

Questa sezione contiene i seguenti argomenti:

Nozioni fondamentali sugli scenari Servizio di controllo (a pagina 295)
Creazione di scenari High Availability per il Servizio di controllo (a pagina 298)
Apertura della Gestione per l'utilizzo dello scenario HA del Servizio di controllo (a pagina 302)
Inversione dei ruoli tra il Servizio di controllo attivo e in stand-by (a pagina 303)

Nozioni fondamentali sugli scenari Servizio di controllo

Il Servizio di controllo funge da unico punto di controllo per le operazioni di Arcserve RHA e contiene tutti i dati degli scenari esistenti. In un sistema di scenario di Arcserve RHA, un Servizio di controllo gestisce tutte le attività correlate agli scenari e le utilità di Gestione collegate consentono di monitorare le attività di Arcserve RHA. Se il Servizio di controllo non è attivo, il funzionamento dello scenario non ne risente. Tuttavia, non è possibile controllare, gestire e monitorare lo stato e il funzionamento degli scenari. Per evitare il rischio di perdere i dati del Servizio di controllo o la possibilità di gestire e monitorare gli scenari, Arcserve RHA dispone degli scenari del Servizio di controllo di Replication e HA. Questi scenari consentono di proteggere i dati e la funzionalità del Servizio di controllo così come vengono protette le altre applicazioni supportate.

Arcserve RHA consente di replicare i dati del Servizio di controllo e salvarli su un host di replica. A tal fine, è necessario creare uno scenario per il Servizio di controllo replica. Lo scenario di replica consente, inoltre, di attivare l'opzione di ripristino e, se necessario, recuperare i dati del Servizio di controllo persi.

Inoltre, Arcserve RHA consente di applicare la soluzione HA al Servizio di controllo. In altre parole, se il Servizio di controllo attivo non è disponibile, è possibile invertire i ruoli del Servizio di controllo attivo e quello in stand-by. Per invertire i ruoli tra due servizi di controllo, è necessario creare uno scenario Servizio di controllo HA.

Importante. Se si sta eseguendo uno scenario per il Servizio di controllo replica, non è possibile utilizzare un secondo Servizio di controllo per gestire le attività correlate agli scenari. Per utilizzare un secondo Servizio di controllo, quando il primo non è disponibile, è necessario installare due servizi di controllo, uno come Servizio di controllo attivo e l'altro come Servizio di controllo in stand-by. Inoltre, è necessario installare due Moduli, uno su ciascun computer dedicato al Servizio di controllo e verificare che siano in esecuzione. Solo così sarà possibile creare ed eseguire uno scenario Servizio di controllo HA.

La creazione di scenari di replica e HA per il Servizio di controllo Arcserve RHA è un processo analogo alla creazione degli scenari di replica e HA per i server applicazioni e di database. In entrambi è possibile utilizzare creazione guidata dello scenario. Ad ogni modo, esistono le seguenti differenze nella creazione di scenari Replication e HA per il Servizio di controllo Arcserve RHA:

- [Scenari di replica e HA] Viene eseguito un solo scenario per Servizio di controllo: è possibile eseguire un solo scenario alla volta per un Servizio di controllo specifico.
- [Scenari di replica e HA] Nessuna licenza speciale richiesta: non è necessario disporre di una particolare licenza per la creazione di uno scenario per il Servizio di controllo replica o HA. Ad ogni modo, è necessario registrare il prodotto Arcserve RHA (a pagina 45) prima di creare uno scenario per il Servizio di controllo.
- [Scenari di replica e HA] Non è possibile modificare i dettagli del server master: nella pagina **Host master e replica** della Creazione guidata scenario, l'indirizzo IP/nome host degli host master e di replica vengono inseriti dall'utente, mentre i dati relativi all'host master sono inseriti automaticamente dal sistema e non possono essere modificati. I dati del Servizio di controllo master visualizzati nella procedura guidata corrispondono ai dati immessi dall'utente nel browser Web per la connessione del Servizio di controllo alla Pagina con informazioni introduttive.

- [Scenario HA] Non è possibile escludere gli elementi del Servizio di controllo dall'applicazione: nella schermata **Configurazione master** nella Creazione guidata scenario, i risultati rilevati automaticamente sono di sola lettura. Non è possibile escludere gli elementi del Servizio di controllo dal processo di replica.
- [Scenario HA] Non è possibile utilizzare il metodo di reindirizzamento IP di spostamento: è possibile utilizzare solo due metodi di reindirizzamento del traffico di rete, Reindirizza DNS e Cambia nome computer. Non è possibile utilizzare il metodo IP di spostamento.
- [Scenario HA] Impossibile disabilitare le funzioni di avanzamento automatico e di replica inversa automatica - quando il server master non è disponibile non è possibile disabilitare l'avvio automatico di un avanzamento e lo scenario precedente. Di conseguenza, la schermata **Avvio replica inversa e di avanzamento** e le relative proprietà non vengono visualizzate o sono disabilitate nella procedura guidata. Tuttavia, è possibile avviare l'avanzamento e la regressione manualmente utilizzando il pulsante **Esegui avanzamento** nella barra degli strumenti standard.
- [Scenario HA] Per creare uno scenario HA per un Servizio di controllo, è necessario installare due servizi di controllo: uno che funga da Servizio di controllo attivo, l'altro come Servizio di controllo in stand-by. Per ulteriori informazioni, consultare la *Guida all'installazione di Arcserve RHA*.

Riferimenti utili:

- Per la creazione di uno scenario per il Servizio di controllo replica, fare riferimento alle istruzioni per la creazione di uno scenario di replica per file server (a pagina 47), unitamente ai requisiti precedentemente indicati.
- Per il ripristino dei dati del Servizio di controllo, fare riferimento al capitolo Recupero di dati e server (a pagina 251).
- Per la creazione di uno scenario Servizio di controllo HA, fare riferimento all'argomento Creazione di uno scenario High Availability per il Servizio di controllo (a pagina 298).
- Per avviare manualmente un avanzamento, fare riferimento all'argomento Avvio manuale dell'avanzamento del Servizio di controllo attivo (a pagina 304).
- Per gestire la perdita di connessione e il processo di avanzamento, fare riferimento all'argomento Processi Avanzamento e Scenario precedente (a pagina 305).
- Per ripristinare lo stato originale dei servizi di controllo, fare riferimento alla sezione Regressione dei ruoli del Servizio di controllo (a pagina 307).

Creazione di scenari High Availability per il Servizio di controllo

Durante la creazione di scenari del Servizio di controllo, Assured Recovery non è supportato e l'opzione non è disponibile.

Importante. Prima di creare uno scenario HA per il Servizio di controllo, verificare che siano stati installati due servizi di controllo, un Servizio di controllo master (attivo) e un Servizio di controllo di replica (stand-by). Il Servizio di controllo di replica dovrebbe essere inattivo. Inoltre, è necessario installare un modulo ed eseguirlo sugli host master e di replica.

Per creare uno scenario High Availability per il Servizio di controllo, procedere come segue:

1. Aprire la Gestione Arcserve RHA. Quindi, dal menu **Scenario** scegliere l'opzione **Nuovo**, oppure fare clic sul pulsante **Nuovo** sulla barra degli strumenti standard.

   Viene visualizzata la **Creazione guidata scenario**.

2. Selezionare le opzioni dello scenario necessarie, come riportate di seguito:
   - Selezionare il pulsante di opzione **Crea nuovo scenario**.
   - Dall'elenco a discesa **Gruppo** selezionare il gruppo a cui assegnare il nuovo scenario. In alternativa, immettere il nome di un nuovo gruppo.

3. Fare clic su **Avanti**. Viene visualizzata la schermata **Selezionare server e tipo di prodotto**.

   Viene presentato un elenco di applicazioni e tipi di scenari disponibili.

   Nota: L'elenco delle applicazioni disponibili dipende dalle licenze applicate**.**

   Selezionare le opzioni dello scenario necessarie, come riportate di seguito:
   - Dall'elenco **Seleziona tipo server**, selezionare **Servizio di controllo**.
   - Dalle opzioni **Seleziona tipo prodotto**, selezionare **Scenario High Availability (HA)**.
   - Si osservi che la Verifica integrità per Assured Recovery non è supportata per scenari HA del Servizio di controllo.

4. Fare clic su **Avanti**. Viene visualizzata la schermata **Host master e replica**.
5. Immettere le seguenti informazioni:
   - Nella casella **Nome scenario** è possibile confermare il nome predefinito oppure immetterne uno nuovo. Quando si immette un nome, scegliere un nome univoco dal momento che non sarà possibile utilizzare lo stesso nome per più scenari.
   - Nella casella **Nome host/IP master**, il sistema inserisce automaticamente il nome host o l'indirizzo IP del Servizio di controllo master (attivo) sulla base dei dati del Servizio di controllo immessi dall'utente per l'apertura della Pagina con informazioni introduttive. Tali dati non possono essere modificati in questa fase. Per utilizzare un Servizio di controllo diverso, è necessario collegarsi alla Pagina con informazioni introduttive, quindi riaprire l'interfaccia Gestione.
   - Nella casella **Nome host/IP di replica**, immettere il nome host o l'indirizzo IP del Servizio di controllo di replica (stand-by) oppure utilizzare i pulsanti **Sfoglia** per trovarli.
   - Nelle caselle **Porta**, accettare il numero di porta predefinito (25000) oppure immettere un nuovo numero di porta per il server master e di replica.

   Note:

   - L'opzione **Modalità di Valutazione** è disabilitata per gli scenari HA.
   - Casella di controllo di **verifica del modulo Arcserve RHA sugli host**: selezionare questa casella se si desidera che il sistema verifichi se i moduli sono installati e in esecuzione sugli host master e di replica specificati in questa pagina. Se i moduli non sono stati installati sugli host selezionati, è possibile utilizzare questa opzione per installare in remoto i moduli su uno o su entrambi gli host. Per ulteriori informazioni sulla pagina di **verifica host**, si rimanda alla sezione Creazione di uno scenario (a pagina 47).
6. Dopo aver selezionato le opzioni desiderate, fare clic su **Avanti**. Viene visualizzata la schermata **Configurazione master**.

   Il componente di rilevamento di Arcserve RHA mostra automaticamente le directory e i file che si trovano sul Servizio di controllo attivo, ovvero le directory e i file relative ai dati che verranno replicati e protetti.

   Gli elementi del Servizio di controllo replicato includono:

   - Registrazione del prodotto: chiavi di registro del prodotto
   - Scenari: file xmc relativi alle definizioni degli scenari
   - Modelli: file xmc relativi ai modelli definiti dall'utente
   - Rapporti: file dei rapporti degli scenari
   - File di configurazione e gestione

Nota: Negli scenari HA del Servizio di controllo, non è possibile escludere gli elementi del Servizio di controllo dalla replica. Negli scenari del Servizio di controllo replica, è possibile escludere gli elementi che non si desidera replicare, deselezionando le relative caselle di controllo.

7. Fare clic su **Avanti**. Viene visualizzata la schermata **Proprietà scenario**.

   Nella schermata **Proprietà scenario** è possibile configurare le proprietà dello scenario che influiscono sull'intero scenario. In genere, i valori predefiniti sono sufficienti.

   Per configurare le proprietà dello scenario in questa fase, consultare la sezione Nozioni fondamentali sulle proprietà dello scenario (a pagina 202). Per configurare le proprietà dello scenario in una fase successiva, consultare la sezione Configurazione delle proprietà dello scenario (a pagina 201).

8. Fare clic su **Avanti**. Viene visualizzata la schermata **Proprietà di master e replica**.

   Nella schermata **Proprietà di master e replica** è possibile configurare le proprietà correlate all'host master o di replica. In genere, i valori predefiniti sono sufficienti.

   Per configurare le proprietà dei server master e di replica in questa fase, consultare la sezione Impostazione delle proprietà del server master e di replica (a pagina 215). Per configurare le proprietà dei server master e di replica in una fase successiva, consultare la sezione Configurazione delle proprietà del server master e di replica (a pagina 216).

   Nota: È possibile modificare tutte le impostazioni in questo riquadro dopo aver creato lo scenario. Tuttavia, prima di modificare le proprietà di spool (che è possibile configurare in questo passaggio), consultare la sezione Spool (a pagina 220) per i dettagli di configurazione.

9. Dopo aver configurato correttamente le proprietà master e di replica, fare clic su **Avanti**.

   Viene visualizzata la finestra **Proprietà avanzamento**:

   La schermata **Proprietà avanzamento** consente di modificare i parametri di avanzamento. Come nei passaggi precedenti, non sono richieste modifiche.

   Per configurare le proprietà dell'avanzamento in questa fase, consultare la sezione Nozioni fondamentali sulle proprietà High Availability (a pagina 273). Per configurare le proprietà dell'avanzamento in una fase successiva, consultare la sezione Configurazione delle proprietà High Availability (a pagina 272).

   Note:

   - Se si seleziona il metodo **Reindirizzamento traffico di rete**, è possibile utilizzare solo due metodi per questo scenario: **Reindirizza DNS** e **Cambia nome computer**. Non è possibile utilizzare il metodo **IP di spostamento**.
   - La proprietà **Timeout per Funzionante (sec)** consente di controllare la durata dell'attesa in seguito al rilevamento di un errore prima dell'attivazione di un avanzamento automatico. Il valore predefinito è 300 secondi. Per ulteriori informazioni, fare riferimento alla sezione Funzionante (a pagina 281).

10. Fare clic su **Avanti**. Viene visualizzato un messaggio di notifica che informa che Arcserve HA verifica la validità del nuovo scenario e controlla i parametri differenti tra i server master e di replica per garantire un corretto avanzamento.

    Nota: In uno scenario Servizio di controllo HA, una volta rilevato un errore dell'host master, vengono avviati sempre automaticamente un processo di avanzamento e uno scenario precedente. L'avvio automatico non può essere disabilitato. Tuttavia, è possibile avviare manualmente un avanzamento, facendo clic sul pulsante **Esegui avanzamento**.

11. Una volta completata la verifica, viene visualizzata la schermata **Verifica scenario**.

12. Se lo scenario non è stato impostato correttamente o se si sono verificati problemi negli host partecipanti o nella connessione tra i componenti di Arcserve RHA, verranno visualizzati i relativi errori e avvisi oltre a due pulsanti aggiuntivi: **Riprova** e **Ulteriori informazioni**.

13. Fare clic sul pulsante **Riprova,** per ripetere il processo di verifica.

14. Fare clic sul pulsante **Ulteriori informazioni,** per visualizzare informazioni aggiuntive sugli errori e gli avvisi.

    Viene visualizzata la finestra di dialogo **Risultati verifica**, in cui sono elencati tutti i messaggi di avviso e di errore.

    La finestra di dialogo **Risultati verifica** include informazioni dettagliate sui controlli eseguiti per la diagnosi dei problemi rilevati. Consente di risolvere eventuali problemi riscontrati durante l'esecuzione del software. Per ulteriore assistenza, rivolgersi al Supporto tecnico.

    - Se vengono visualizzati errori, non è possibile eseguire lo scenario. È necessario correggere questi errori prima di poter avviare i processi di sincronizzazione, replica e HA.
    - Se vengono visualizzati solo messaggi di avviso, è possibile eseguire lo scenario. Tuttavia, è importante tenere conto dell'avviso in quanto indica condizioni che potrebbero potenzialmente provocare problemi di replica o avanzamento. Per chiudere la finestra di dialogo e tornare alla schermata **Verifica scenari**, fare clic sul pulsante **Annulla**.
    - Se la verifica dello scenario non presenta errori, nella schermata **Verifica scenari** fare clic su **Avanti** per continuare.

    Viene visualizzata la schermata **Esecuzione scenario**.

15. Al termine della configurazione dello scenario, verrà richiesto di eseguirlo. L'esecuzione dello scenario consente di avviare il processo di sincronizzazione dei dati, seguito dalle verifiche Funzionante e di replica.

    - Per completare la creazione dello scenario ed eseguirlo in seguito, selezionare **Fine**.
    - Per eseguire il processo, selezionare **Esegui ora**.

16. Viene avviato il processo di sincronizzazione. Il processo di sincronizzazione potrebbe richiedere del tempo, a seconda della dimensione dei dati e della larghezza di banda della rete tra server master e di replica. Quando la sincronizzazione sarà completata, si riceverà il seguente messaggio nel riquadro Eventi: **Tutte le modifiche avvenute durante il periodo di sincronizzazione sono state replicate**.

    Da questo punto, verrà eseguita la replica in tempo reale e la soluzione ad alta disponibilità sarà attiva.

Apertura della Gestione per l'utilizzo dello scenario HA del Servizio di controllo

Per utilizzare correttamente lo scenario Servizio di controllo HA, è importante visualizzare la Pagina con informazioni introduttive e da questa la Gestione, utilizzando il nome host del Servizio di controllo anziché il relativo indirizzo IP. Se si desidera utilizzare l'indirizzo IP del Servizio di controllo, dopo l'esecuzione di un avanzamento Arcserve RHA non sarà più in grado di connettere automaticamente la Pagina con informazioni introduttive e la Gestione al nuovo Servizio di controllo attivo.

Inoltre, se si intende utilizzare lo scenario Servizio di controllo HA, NON avviare la Gestione dal computer in cui è installato il Servizio di controllo. Avviare invece la Gestione da un terzo computer, che non agisce come Servizio di controllo attivo o in stand-by.

Per aprire la Gestione di Arcserve RHA e utilizzare lo scenario HA del Servizio di controllo.

1. Aprire Internet Explorer. Nella casella **Indirizzo**, immettere il nome host e il numero di porta del Servizio di controllo utilizzando il seguente formato: http://nome_host:numero_porta/pagina_iniziale.aspx

    Nota: se durante l'installazione del Servizio di controllo si è selezionata l'opzione **Configurazione SSL,** immettere il nome host e il numero di porta del Servizio di controllo utilizzando il seguente formato: \https://nome_host:numero_porta/pagina_iniziale.aspxx

    Viene visualizzata la finestra di dialogo **Accesso.**

2. Immettere nome utente, password e dominio, quindi fare clic sul pulsante **Accedi**.

    Viene visualizzata la **Pagina con informazioni introduttive**.

3. Nella barra degli strumenti **Avvio rapido** a sinistra, fare clic sull'opzione **Gestione scenario**.

    Viene visualizzata una barra di avanzamento che indica che il componente Gestione è attualmente installato nel computer locale.

4. Al termine del processo di installazione la Gestione viene avviata.

   È ora possibile iniziare la creazione dello scenario Servizio di controllo HA (a pagina 298).

Inversione dei ruoli tra il Servizio di controllo attivo e in stand-by

L'arresto di un Servizio di controllo, intenzionale o anomalo, presenta un unico problema: la Pagina con informazioni introduttive e il componente Gestione vengono disconnessi. Di conseguenza non possono ricevere informazioni aggiornate né visualizzare un'indicazione visiva del tipo di evento che si è verificato. Sebbene la Pagina con informazioni introduttive e il componente Gestione siano attivi, non è possibile rilevare che il Servizio di controllo non lo è, pertanto non sarà possibile avviare manualmente un avanzamento in questa fase.

Arcserve RHA gestisce il problema della disconnessione tentando di ripristinare automaticamente lo stato attivo del Servizio di controllo (Gestione). Se il tentativo non riesce e il Servizio di controllo rimane non attivo, Arcserve RHA avvia automaticamente l'avanzamento. Durante questo processo, il Servizio di controllo in stand-by diventa il Servizio di controllo attivo. Di conseguenza la Pagina con informazioni introduttive e il componente Gestione vengono automaticamente riconnessi al nuovo Servizio di controllo attivo e visualizzeranno nuovamente lo stato aggiornato del sistema. Mentre viene ristabilita la connessione, all'utente viene richiesto di rieseguire l'accesso.

Quando il Servizio di controllo attivo originale è nuovamente attivo, Arcserve RHA avvia automaticamente uno scenario precedente. Lo scenario precedente è una replica nella direzione inversa: dal nuovo server del Servizio di controllo attivo al nuovo server del Servizio di controllo in stand-by. A questo punto è possibile invertire i ruoli dei servizi di controllo. È sufficiente avviare manualmente una regressione, ovvero un avanzamento nella direzione opposta.

Oltre all'avanzamento automatico predefinito, è anche possibile avviare manualmente un avanzamento tra i servizi di controllo attivi e in stand-by. Una volta attivato, manualmente o automaticamente, il processo di avanzamento stesso è completamente automatizzato.

Il processo di inversione dei ruoli dei Servizi di controllo attivi e in stand-by prevede diverse fasi:

1. Avvio di un avanzamento (a pagina 304): questa operazione può essere eseguita automaticamente dal sistema, quando viene rilevato lo stato non attivo del Servizio di controllo, oppure manualmente dall'utente.
2. Esecuzione del processo di avanzamento e avvio automatico dello scenario precedente (a pagina 305): questi processi vengono eseguiti automaticamente e non è possibile disabilitarli.
3. Avvio di una regressione (a pagina 307): questa operazione può essere eseguita manualmente solo dall'utente, nel momento in cui decide che il Servizio di controllo attivo originario può essere nuovamente impostato come server attivo.

Avvio manuale dell'avanzamento del Servizio di controllo attivo

Una volta che Arcserve RHA rileva che il Servizio di controllo attivo non è più attivo, tenta di riavviare automaticamente il Servizio di controllo e, se il tentativo non riesce, avvia un avanzamento. Tuttavia può anche avviare un avanzamento manuale, quando il Servizio di controllo attivo è ancora in esecuzione.

Nota: Non eseguire il Servizio di controllo sugli host master e di replica allo stesso tempo al fine di evitare errori imprevisti, come ad esempio l'interruzione della connessione.

Per avviare l'avanzamento manualmente, procedere come segue:

1. Aprire la Gestione e selezionare il Servizio di controllo desiderato dal riquadro Scenario. Verificare che lo scenario sia in esecuzione.
2. Fare clic sul pulsante **Esegui avanzamento** oppure scegliere l'opzione **Esegui avanzamento** dal menu **Strumenti**:

   Verrà visualizzato un messaggio di conferma.
3. Fare clic su **Sì** nella finestra di conferma **Esegui avanzamento**. Questa procedura consente di avviare un avanzamento dal Servizio di controllo attivo al Servizio di controllo in stand-by.

   In questa fase, il processo di avanzamento (a pagina 305) è lo stesso per l'avvio manuale e automatico.

Processi Avanzamento e Scenario precedente

Nozioni fondamentali sui processi Avanzamento e Scenario precedente

1. Poiché il Servizio di controllo attivo originario non è attivo, la Pagina con informazioni introduttive e la Gestione non vi sono più connessi. Pertanto, non possono più ricevere e visualizzare informazioni aggiornate e di conseguenza non includono le modifiche applicate dopo l'avvio dell'avanzamento, in quanto queste vengono visualizzate in un avanzamento normale.
2. Quando la Pagina con informazioni introduttive perde la connessione al Servizio di controllo attivo originario, viene visualizzato il seguente messaggio.

   Questo messaggio indica che il Servizio di controllo attivo originario non è attivo, pertanto non è più connesso alla Pagina con informazioni introduttive.
3. Fare clic su **OK** per chiudere il messaggio. È possibile che questo messaggio venga visualizzato più volte fino a quando il Servizio di controllo in stand-by non diventa attivo e viene stabilita una connessione.
4. Quando il Servizio di controllo in stand-by originario è attivo e in esecuzione come nuovo Servizio di controllo attivo, la Pagina con informazioni introduttive viene automaticamente riconnessa e viene visualizzata la finestra di dialogo **Accesso** in cui viene richiesto di accedere al nuovo Servizio di controllo attivo.
5. Immettere nome utente, password e dominio, quindi fare clic sul pulsante **Accedi**.

   Viene nuovamente visualizzata la **Pagina con informazioni introduttive**, che sarà ora connessa al nuovo Servizio di controllo attivo.
6. Nella Gestione, potrebbe essere visualizzata la finestra di dialogo **Credenziali utente**.

   In questa finestra viene richiesto di accedere al nuovo Servizio di controllo attivo. Se viene visualizzata questa finestra di dialogo, immettere i dettagli necessari e fare clic **OK**.

   Nota: la visualizzazione della finestra di dialogo **Credenziali utente** è correlata alle impostazioni di inserimento nella cache interne e non è necessaria alcuna indicazione al progresso del processo di avanzamento. L'avanzamento può essere eseguito anche se questa finestra di dialogo non è visualizzata.
7. I due servizi di controllo hanno regredito i ruoli. Ora, la Gestione non è più connessa al Servizio di controllo attivo originario, bensì al Servizio di controllo in stand-by, che diventa attivo in seguito all'avanzamento. Gli eventi correlati all'avanzamento vengono visualizzati nel riquadro Evento.

Nota: problema e la soluzione Split Brain":

Dopo la perdita della connessione e un avanzamento, il Servizio di controllo in stand-by originario funziona come Servizio di controllo attivo. Tuttavia, il Servizio di controllo attivo originario potrebbe ancora essere in esecuzione. Una volta ristabilita la connessione, entrambi i servizi di controllo attivi potrebbero tentare di agire come Servizio di controllo attivo. Per risolvere questo possibile problema, Arcserve RHA mantiene il parametro numerico incorporato in ciascun Servizio di controllo e il processo di avanzamento aumenta il numero del Servizio di controllo appena attivato. Tutte le richieste di connessione vengono inviate a questo parametro e quando il Servizio di controllo riceve una richiesta, verifica se contiene un numero inferiore o superiore a quello che trasporta. Il Servizio di controllo attivo che trasporta il numero più basso, si interrompe e diventa il Servizio di controllo in stand-by.

8. Dopo l'avanzamento, viene avviato automaticamente uno scenario precedente.
9. Lo scenario precedente inizia a essere eseguito dopo che il Servizio di controllo attivo originario è in esecuzione. Questo consente di replicare i dati dal nuovo Servizio di controllo attivo al nuovo Servizio di controllo in stand-by, sovrascrivendo contemporaneamente quelli presenti nel Servizio di controllo in stand-by corrente.
10. È ora possibile eseguire la regressione dei ruoli del Servizio di controllo attivo e in stand-by (a pagina 307) e rendere il server master originario nuovamente il server attivo e il server di replica il server in stand-by.

Regressione dei ruoli del Servizio di controllo

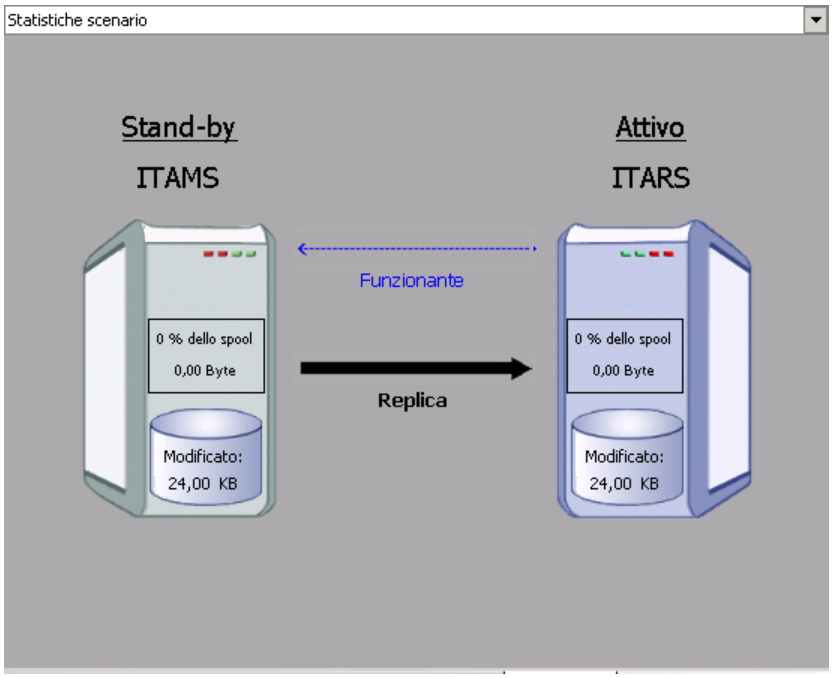
Quando il Servizio di controllo attivo originario è di nuovo attivo e lo scenario precedente è in esecuzione, è possibile eseguire la regressione dei ruoli del Servizio di controllo in stand-by e attivo e riportarli allo stato originario.

Per avviare una regressione, procedere come segue:

1. Per riportare i ruoli dei servizi di controllo allo stato originario quando lo scenario precedente è in esecuzione, fare clic sul pulsante **Esegui avanzamento** oppure scegliere l'opzione **Esegui avanzamento** dal menu **Strumenti**.

   Viene visualizzato un messaggio di conferma.

2. Fare clic su **Sì** nella finestra di conferma **Esegui avanzamento**. Questa procedura consente di avviare una regressione dal server di replica originario al server master. Ancora una volta non sarà possibile visualizzare il processo di regressione sulla Pagina con informazioni introduttive e la Gestione, in quanto sono entrambi disconnessi dal Servizio di controllo attivo. Una volta che la Pagina con informazioni introduttive e la Gestione sono di nuovo connesse, si noterà che i servizi di controllo hanno riportato i ruoli agli stati originari.



   Ora, lo scenario Servizio di controllo HA sarà in esecuzione nella direzione originaria.

Capitolo 12: Verifica Assured Recovery

In questo capitolo viene illustrata l'opzione di verifica per il Assured Recovery e vengono descritte le seguenti operazioni: creazione di uno scenario Assured Recovery, esecuzione di una verifica per Assured Recovery in modalità pianificata e non pianificata e configurazione delle proprietà di Assured Recovery. Viene inoltre descritta la modalità di impostazione della creazione e di gestione di snapshot VSS.

Questa sezione contiene i seguenti argomenti:

Informazioni su Assured Recovery (a pagina 309)
Creazione di uno scenario di verifica Assured Recovery (a pagina 311)
Configurazione delle proprietà Assured Recovery (a pagina 314)
Impostazione delle proprietà di Assured Recovery (a pagina 316)
Esecuzione di una verifica Assured Recovery (a pagina 319)

Informazioni su Assured Recovery

L'opzione Assured Recovery consente di eseguire una verifica trasparente completa della recuperabilità dei dati sul server di replica. Il server di replica che viene testato è quello che subentrerebbe al server di produzione qualora questo non fosse attivo. L'opzione Assured Recovery è una verifica effettiva del server reale, delle applicazioni e delle azioni che saranno necessarie nel caso in cui il server di replica dovesse diventare il server attivo e svolgerne le relative funzioni.

La verifica Assured Recovery viene eseguita avviando i servizi di database ed effettuando qualsiasi operazione richiesta per la verifica dell'integrità dei dati. Tutto questo è possibile senza la necessità di eseguire la risincronizzazione e senza influire sulla disponibilità del server di produzione o sulla protezione fornita dai sistemi di replica e HA.

Durante il test, le continue modifiche dei dati sul server master vengono inviate al server di replica, ma non vengono immediatamente applicate. Tali modifiche vengono piuttosto accumulate e memorizzate in uno spool, e verranno applicate ai dati del server di replica solo al completamento del test. Poiché lo spool viene eseguito sul server di replica, se accade qualcosa al server master durante il processo di test nessuna delle modifiche accumulate andrà perduta.

Al termine del test, l'opzione Assured Recovery interrompe i servizi applicativi che aveva avviato sul server di replica. Quindi, il server di replica viene ripristinato in automatico allo stato esistente al momento della sospensione della replica e viene avviato il test. In tal modo, sarà possibile applicare le modifiche accumulate nello spool come se non fosse stato eseguito alcun test. Da questo punto in poi, la replica o lo scenario HA riprende il normale funzionamento. Nel caso di uno scenario HA, se si verifica un errore sul master durante il test, l'avanzamento viene riavviato.

La verifica Assured Recovery può essere completamente automatizzata ed eseguita su base pianificata, con la frequenza desiderata. Al termine, sarà possibile avvisare il personale appropriato dello stato della verifica e attivare ulteriori azioni in caso di riuscita; ad esempio, scattare una snapshot (istantanea) VSS dei dati del server di replica oppure creare un backup. Inoltre, sarà possibile eseguire la verifica Assured Recovery in modalità non pianificata quando necessario.

La verifica Assured Recovery è personalizzatain base a tutte le applicazioni e ai server di database supportati. Tuttavia, dal momento che l'opzione Assured Recovery esegue il test dei servizi di database, non è completamente applicabile ai file server e ai server IIS. È comunque possibile utilizzare l'opzione Assured Recovery con questi server per attività speciali. Ad esempio, è possibile sospendere automaticamente la replica a intervalli periodici durante alcune ore di ogni giorno, settimana o mese, ed eseguire script durante tale intervallo, oppure approfittare di questa sospensione per acquisire snapshot VSS sul server di replica. Dal momento che non esiste un'*applicazione* di per sé, la verifica dei dati con scenari file server e server IIS richiede ulteriori script personalizzati.

L'opzione Assured Recovery supporta sia le soluzioni Replication che High Availability, con eccezione degli scenari del Servizio di Controllo. È tuttavia più adeguata a scenari HA poiché, in questo caso, il server di replica contiene necessariamente i server di database reali, sui quali viene eseguito il test, e non semplicemente i dati.

Nota: l'opzione Assured Recovery non è disponibile per gli scenari del Servizio di controllo.

Se si utilizza la verifica Assured Recovery come parte di uno scenario di replica, verificare che il percorso delle directory principali del master e della replica coincidano. In aggiunta, sul server di replica dovrebbe essere installata un'applicazione di database oppure, se si esegue il test di un file server, dovrebbero essere condivisi file che dovranno essere configurati sui server master e di replica esattamente allo stesso modo. In caso contrario, la verifica Assured Recovery non produrrà risultati significativi.

Creazione di uno scenario di verifica Assured Recovery

La funzione di verifica per Assured Recovery deve essere abilitata durante la creazione dello scenario che la utilizzerà in seguito. Per questo motivo, non è possibile eseguire test nell'ambito di uno scenario di replica o HA già in esecuzione e non configurato per l'utilizzo dell'opzione Assured Recovery. Per utilizzare Assured Recovery, è necessario creare un nuovo scenario con l'opzione Verifica integrità per Assured Recovery attivata.

Nota: in questa sezione viene illustrata la creazione di uno scenario di verifica Assured Recovery per HA di Exchange Server. La procedura è simile per tutti i tipi d'applicazione.

Per impostare uno scenario di verifica Assured Recovery, procedere come segue:

1. Aprire la Gestione Arcserve RHA. Quindi, dal menu Scenario selezionare l'opzione Nuovo oppure fare clic sul pulsante Nuovo sulla barra degli strumenti standard.

   Viene visualizzata la Creazione guidata scenario.

2. Selezionare le opzioni dello scenario necessarie, come riportate di seguito:

   - Selezionare il pulsante di opzione Crea nuovo scenario.
   - Dall'elenco a discesa Gruppo selezionare il gruppo a cui assegnare il nuovo scenario. In alternativa, immettere il nome di un nuovo gruppo.

3. Fare clic su Avanti. Viene visualizzata la schermata Selezionare server e tipo di prodotto.

4. Viene presentato un elenco di applicazioni e tipi di scenari disponibili.

   Nota: l'elenco di applicazioni disponibili dipende dalle licenze applicate**.**

   Selezionare le opzioni dello scenario necessarie, come riportate di seguito:

   - Dall'elenco Seleziona tipo server, selezionare il tipo di server per il quale si desidera creare lo scenario. In questo esempio, verrà utilizzato Microsoft Exchange Server.
   - Dalle opzioni Seleziona tipo prodotto, selezionare lo scenario Replication e Disaster Recovery oppure lo scenario High Availability.

     Nota: la verifica per Assured Recovery testing è l'opzione adeguata agli scenari HA. Se si seleziona l'opzione Replica, verificare che il percorso delle directory principali del master e della replica coincidano. In aggiunta, sul server di replica dovrebbe essere installata un'applicazione di database oppure dovrebbero essere condivisi file se si esegue il test di un file server. In caso contrario, la verifica Assured Recovery NON produrrà risultati significativi.

   - Selezionare l'opzione Verifica di integrità per Assured Recovery.

5. Fare clic su **Avanti**. Viene visualizzata la schermata Host master e replica.
6. Immettere le seguenti informazioni:
   - Nella casella Nome scenario è possibile confermare il nome predefinito oppure immetterne uno nuovo. Quando si immette un nome, scegliere un nome univoco dal momento che non sarà possibile utilizzare lo stesso nome per più scenari.
   - Nelle caselle Nome host/IP master e Nome host/IP di replica, immettere il nome host o l'indirizzo IP dei server master (attivo) e di replica (in stand-by) oppure utilizzare i pulsanti Sfoglia per trovarli.

   Importante. È possibile configurare un solo server di replica per la verifica Assured Recovery in un unico scenario. Se, in un secondo momento, si decide di aggiungere un server di replica allo scenario e si tenta di configurarlo per la verifica Assured Recovery, verrà visualizzato il seguente messaggio: **È possibile impostare solo un'attività pianificata per scenario. Verifica di integrità di replica per Assured Recovery è già impostato su ATTIVO per l'host [nome_server_di_replica]. DISATTIVARE l'opzione ora?** Per attivare il test sul secondo server di replica fare clic su Sì.

   Nota: se un server è un cluster MSCS, immettere il nome del server virtuale oppure l'indirizzo IP come nome del server master e/o di replica (invece del nome/IP del nodo fisico).

   - Nelle caselle Porta, accettare il numero di porta predefinito (25000) oppure immettere i nuovi numeri di porta per il server master e di replica.
   - Opzione di verifica del modulo sugli host: selezionare questa casella di controllo affinché il sistema verifichi se i moduli sono installati e in esecuzione sugli host master e di replica specificati in questa schermata. Se i moduli non sono stati installati sugli host selezionati, è possibile utilizzare questa opzione per installare in remoto i moduli su uno o su entrambi gli host.
7. Dopo aver immesso o selezionato le opzioni desiderate, fare clic su Avanti. Viene visualizzata la schermata dei database per la replica

   Il componente di rilevamento automatico mostra automaticamente i database di Exchange che si trovano sul server master. Questi sono i database che è possibile replicare e proteggere.
8. Per impostazione predefinita, tutti i database rilevati verranno selezionati e quindi replicati. Per escludere qualsiasi gruppo di archiviazione dalla replica, deselezionare la relativa casella di controllo.

9. Fare clic su Avanti. Verrà visualizzata la schermata Configurazione di replica.

   Il componente di configurazione automatica verifica che la configurazione di Exchange Server sui server master e di replica resti invariata durante la procedura di replica. Ciò significa che qualora vi fossero delle discrepanze, Arcserve RHA eseguirà le azioni richieste, tra cui: creazione, modifica o eliminazione di gruppi di archiviazione, cartelle pubbliche e archivi di caselle di posta elettronica dal server di replica. Le operazioni che verranno eseguite durante il processo di configurazione sono indicate nella colonna Azione a destra.

10. Esaminare le modifiche che verranno apportate durante la configurazione automatica sul server Exchange di replica e assicurarsi che siano di proprio gradimento.

    Nota: se viene indicata un'azione di rimozione, è necessario essere sicuri di voler procedere all'eliminazione dell'elemento di archiviazione specificato dal server di replica, in quanto esso non dispone di un backup automatico. Se si desidera salvarlo in una diversa posizione prima dell'eliminazione, fare clic sul pulsante Fine per uscire dalla procedura guidata.

    Importante. Non è possibile utilizzare i percorsi UNC come directory principali sull'host di replica per lo scenario Assured Recovery.

11. Fare clic su **Avanti** per avviare il processo di configurazione del server di replica. Viene visualizzata la schermata Proprietà scenario.

    Nella schermata **Proprietà scenario** è possibile configurare le proprietà dello scenario che influiscono sull'intero scenario. In genere, i valori predefiniti sono sufficienti.

    Per configurare le proprietà dello scenario in questa fase, consultare la sezione Nozioni fondamentali sulle proprietà dello scenario (a pagina 202). Per configurare le proprietà dello scenario in una fase successiva, consultare la sezione Configurazione delle proprietà dello scenario (a pagina 201).

12. Fare clic su Avanti. Viene visualizzata la schermata Proprietà di master e replica.

    In questa schermata è possibile configurare le proprietà correlate all'host master o di replica. In genere, i valori predefiniti sono sufficienti.

13. Per verificare che l'opzione Assured Recovery sia attiva, nell'elenco Proprietà di replica a destra, aprire il gruppo Attività pianificate e assicurarsi che la proprietà Verifica di integrità di replica per Assured Recovery sia impostata su Attivo. È possibile lasciare invariati i valori predefiniti delle altre proprietà correlate e modificarli in seguito, se necessario. Per ulteriori informazioni sulle proprietà di Assured Recovery, consultare la sezione Nozioni fondamentali delle proprietà di Assured Recovery (a pagina 316).

    Per configurare le proprietà dei server master e di replica in questa fase, consultare la sezione Impostazione delle proprietà del server master e di replica (a pagina 215). Per configurare le proprietà dei server master e di replica in una fase successiva, consultare la sezione Configurazione delle proprietà del server master e di replica (a pagina 216).

Nota: è possibile modificare tutte le impostazioni in questo riquadro dopo aver creato lo scenario. Tuttavia, prima di modificare le proprietà di spool (che è possibile configurare in questo passaggio), consultare la sezione Spool (a pagina 220) per i dettagli di configurazione.

14. Fare clic su Avanti. Se è stata selezionata la soluzione HA, viene visualizzata la schermata Proprietà avanzamento.
15. Procedere quindi all'impostazione dello scenario secondo la normale procedura. Per ulteriori informazioni, consultare la Guida operativa appropriata. Una volta completata la creazione dello scenario, eseguire lo scenario.

    Quando la sincronizzazione iniziale sarà stata completata e il processo di replica è attivo, sarà possibile eseguire la verifica Assured Recovery.

Configurazione delle proprietà Assured Recovery

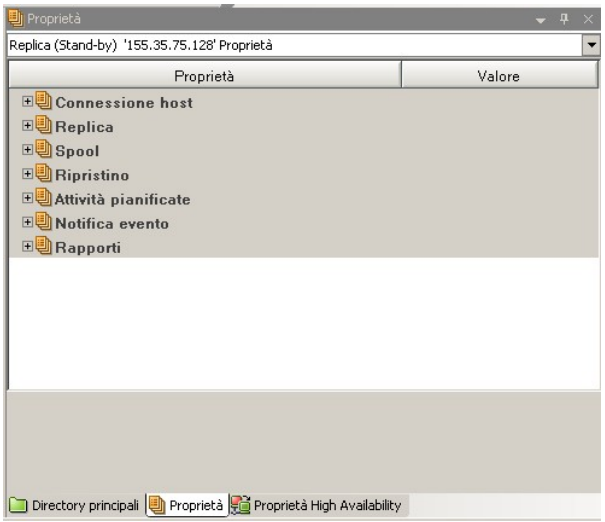
Per configurare le proprietà Assured Recovery, è necessario interrompere lo scenario.

Nota: il riquadro Proprietà e le relative schede (Directory principali, Proprietà, Statistiche) sono basati sul contesto e vengono modificati tutte le volte che si seleziona un nodo diverso da una cartella di scenari.

Per impostare le proprietà di uno scenario Assured Recovery, procedere come segue:

1. Dal riquadro Scenario, selezionare il server di replica che si desidera sottoporre al test e le cui proprietà si desidera configurare.
2. Nel riquadro Struttura selezionare la scheda Statistiche.

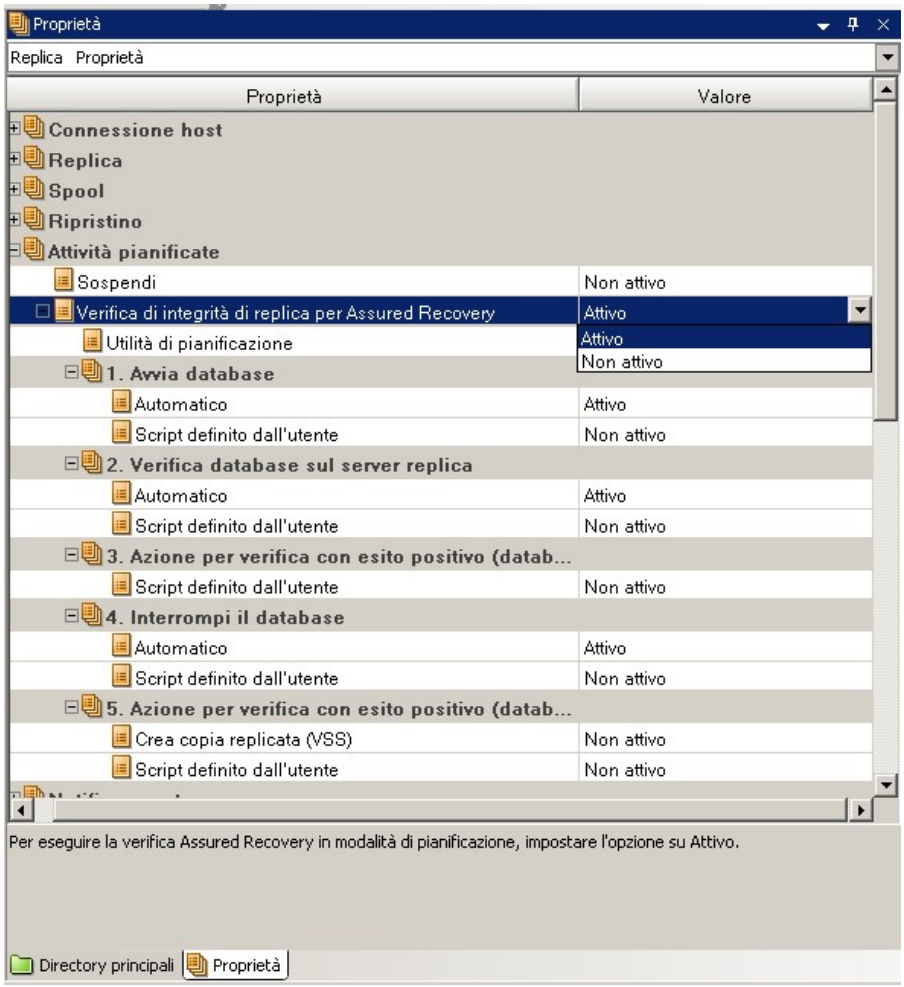
   Viene visualizzato l'elenco Proprietà di replica.



Nota: uno scenario in esecuzione ha lo sfondo di colore grigio, mentre gli scenari non in esecuzione hanno uno sfondo di colore bianco.

3. Se lo scenario è in esecuzione, fare clic sul pulsante Interrompi sulla barra degli strumenti. Lo scenario viene interrotto.

4. Nell'elenco delle proprietà del server di replica, aprire il gruppo Attività pianificate per visualizzare le proprietà della Verifica di integrità di replica per Assured Recovery.



5. Nell'elenco, selezionare la proprietà richiesta e selezionare o immettere i valori appropriati. È possibile selezionarne alcuni valori da una casella combinata e immetterne altri manualmente nel campo di una casella di modifica.

6. Fare clic sul pulsante Salva sulla barra degli strumenti standard per salvare e applicare le modifiche.

Impostazione delle proprietà di Assured Recovery

In questa sezione vengono elencate le proprietà di Assured Recovery, i valori corrispondenti e una spiegazione per ciascuna proprietà.

Nota: sui sistemi Windows a 64 bit, non è possibile eseguire gli script che attivano applicazioni con un'interfaccia grafica utente.

Utilità di pianificazione

L'utilità di pianificazione consente di eseguire automaticamente le verifiche Assured Recovery in base ad una pianificazione predefinita, ad esempio a intervalli di ore, una volta al giorno o varie volte al mese. Per l'impostazione dell'utilità di pianificazione, si rimanda alla sezione Esecuzione della verifica Assured Recovery in modalità non pianificata (a pagina 320).

Avvia DB

Questa proprietà definisce il primo passaggio della verifica Assured Recovery: l'avvio dei servizi di database sul server di replica.

Automatico

L'impostazione predefinita della proprietà è Attivo. Per utilizzare uno script in modo da sostituire l'avvio automatico dei servizi di database, disattivare questa opzione.

Script definito dall'utente

È possibile specificare uno script per aumentare o sostituire il passaggio standard per l'avvio di servizi di database.

Per sostituire il passaggio standard, impostare **Automatico** su Non attivo e **Script definito dall'utente** su Attivo. Quindi, specificare il nome del percorso completo dello script da eseguire nella casella **Nome script**.

Per eseguire lo script in base al passaggio standard, lasciare attivata l'opzione **Automatico**.

Nome script (percorso completo)

Immettere il nome e il percorso completo dello script che viene richiamato in seguito all'avvio dei servizi di database o in suo luogo.

Argomenti

Argomenti aggiuntivi da trasmettere allo script, specificato nella proprietà precedente. Gli argomenti immessi in questa sezione sono valori statici.

Verifica database sul server di replica

Questa proprietà definisce la seconda fase della verifica Assured Recovery: la verifica del corretto avvio di tutti i servizi di applicazione, il corretto montaggio di tutti i database e archivi delle informazioni, oltre che della validità del loro stato.

Automatico

L'impostazione predefinita della proprietà è Attivo. Per utilizzare uno script in modo da sostituire le azioni automatiche eseguite durante la fase di convalida di questo database, disattivare questa opzione.

Script definito dall'utente

È possibile specificare uno script per aumentare o sostituire le azioni eseguite durante la fase di convalida di questo database.

Per sostituire il passaggio standard, impostare Automatico su Non attivo e Script definito dall'utente su Attivo. Quindi, specificare il nome del percorso completo dello script da eseguire nella casella Nome script.

Per eseguire lo script in base al passaggio standard, lasciare attivata l'opzione Automatico.

Nome script (percorso completo) -- Immettere il nome e il percorso completo dello script richiamato successivamente alla fase di convalida del database o in sostituzione di questa.

Argomenti -- Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Gli argomenti immessi in questa sezione sono valori statici.

Azione in caso di verifica con esito positivo (database in linea)

Dopo aver testato correttamente il server di replica, i dati applicativi si trovano in uno stato noto e valido. Ciò potrebbe essere utile, ad esempio, ad assicurarsi che a questo punto venga eseguito un backup su dati convalidati. Se l'azione che si desidera eseguire richiede che l'applicazione sia in esecuzione e che i database o gli archivi informazioni siano montati, sarà opportuno registrarla tramite uno script in questo passaggio, specificando i dettagli dello script nelle caselle Script definito dall'utente. In questa sezione non sono previste azioni predefinite.

Script definito dall'utente

Nome script (percorso completo) -- Immettere il nome e il percorso completo dello script richiamato quando l'applicazione è ancora in esecuzione e i database o gli archivi delle informazioni sono montati.

Argomenti -- Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Gli argomenti immessi in questa sezione sono valori statici.

Interrompi il database

Questa proprietà definisce il terzo e ultimo passaggio di una verifica Assured Recovery standard: l'interruzione dei servizi di database al termine del test.

Automatico

L'impostazione predefinita della proprietà è Attivo. Per utilizzare uno script in modo da sostituire l'interruzione automatica dei servizi di database, impostare questa opzione su Non attivo.

Script definito dall'utente

È possibile specificare uno script per aumentare o sostituire il passaggio standard per l'interruzione di servizi di database.

- Per sostituire il passaggio standard, impostare **Automatico** su Non attivo e **Script definito dall'utente** su Attivo. Quindi, specificare il nome del percorso completo dello script da eseguire nella casella **Nome script**.
- Per eseguire lo script in base al passaggio standard, lasciare attivata l'opzione **Automatico**.

Nome script (percorso completo) -- Immettere il nome e il percorso completo dello script richiamato successivamente alla fase di interruzione dei servizi del database o in sostituzione di questa.

Argomenti -- Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà precedente. Gli argomenti immessi in questa sezione sono valori statici.

Azioni in caso di esito positivo della verifica (database non in linea)

Come indicato in Actions upon Successful Test (DB Online) (Azioni in caso di esito positivo della verifica (database in linea), in questa fase l'applicazione si trova in uno stato valido. Se lo si desidera, è ora possibile eseguire una copia, il backup o acquisire una snapshot. Se l'azione non richiede che l'applicazione sia in esecuzione, registrarla in questo passaggio mediante uno script, specificando il nome completo del percorso di uno script nel campo Script definito dall'utente.

Nota: su Windows Server 2003 e sistemi successivi, è possibile generare snapshot VSS in modo automatico. Per ulteriori informazioni, consultare la sezione Creazione automatica di snapshot VSS (a pagina 327).

Script definito dall'utente

Nome script (percorso completo) -- Immettere il nome e il percorso completo dello script che viene richiamato dopo il completamento della verifica Assured Recovery.

Argomenti -- Argomenti aggiuntivi da trasmettere allo script specificato nella proprietà Nome script. Gli argomenti immessi in questa sezione sono valori statici.

Limiti della verifica Assured Recovery

Durante l'esecuzione della verifica Assured Recovery con Oracle o database SQL server, il software non verifica se il database è già stato montato. Viene solo verificato se il servizio è in esecuzione. È possibile creare uno script personalizzato che confermi che entrambi i servizi sono in esecuzione che i database sono stati montati. Abilitare la proprietà appropriata per lo script definito dall'utente. Consultare la sezione Nozioni fondamentali delle proprietà di Assured Recovery (a pagina 316) per maggiori informazioni.

Esecuzione di una verifica Assured Recovery

La verifica Assured Recovery può essere completamente automatizzata ed eseguita su base pianificata, con la frequenza desiderata. Al termine, sarà possibile avvisare il personale appropriato dello stato del test e attivare ulteriori azioni in caso di riuscita; ad esempio, scattare una snapshot (istantanea) VSS dei dati oppure eseguire un backup. In alternativa, sarà possibile eseguire il test in modalità non pianificata, avviandolo automaticamente o manualmente quando necessario.

In entrambe le modalità, la verifica Assured Recovery viene eseguita in passaggi stabiliti nelle relative impostazioni di configurazione. Alcuni dei passaggi sono trasparenti e vengono eseguiti automaticamente ogni volta che viene eseguita una verifica Assured Recovery. Altri passaggi sono visibili ed è possibile configurarne l'eventualità e la modalità di esecuzione.

I passaggi standard sono i seguenti:

1. Avvio della verifica Assured Recovery - Fare clic sul pulsante di verifica di integrità di replica nella barra degli strumenti per avviare la verifica Assured Recovery in modalità pianificata o non pianificata.
2. Sospensione dell'applicazione delle modifiche dei dati sul server di replica testato - Questo passaggio viene eseguito automaticamente all'inizio di ogni verifica Assured Recovery.
3. Avvio di un componente di ripristino sul server di replica testato - Questo passaggio viene eseguito automaticamente. Lo scopo è quello di acquisire tutte le modifiche apportate ai dati del server di replica durante il test, in modo che in seguito sia possibile ripristinarli a partire dal punto in cui la replica era stata sospesa.
4. Avvio dei servizi di database - Per impostazione predefinita, questo passaggio viene eseguito automaticamente. Ad ogni modo, è possibile disattivarlo, sostituirlo oppure farlo seguire da uno script definito dall'utente.

5. Test del database - Per impostazione predefinita, i database vengono verificati mediante gli stessi test utilizzati per monitorare il database in HA. Questi test includono la verifica del corretto avvio di tutti i servizi e che i database siano stati montati correttamente. Questi test possono essere disattivati, sostituiti o seguiti da uno script definito dall'utente.
6. Esecuzione di azioni in caso di esito positivo della verifica durante i servizi di database - In caso di esito positivo della verifica, è possibile registrare uno script definito dall'utente per eseguire le azioni desiderate e per le quali è necessario che l'applicazione sia in esecuzione.
7. Interruzione dei servizi di database - Per impostazione predefinita, questo passaggio viene eseguito automaticamente. Ad ogni modo, è possibile disattivarlo, sostituirlo oppure farlo seguire da uno script definito dall'utente.

   Esecuzione di ulteriori azioni in caso di esito positivo della verifica mentre i servizi di database sono interrotti - Questo passaggio è facoltativo e può essere utilizzato per eseguire azioni basate sul superamento dei test di convalida e sull'interruzione in ordine sistematico dell'applicazione.
8. Ripristino dei dati di replica Assured Recovery e ripresa della replica - Questo passaggio viene eseguito automaticamente al termine di ogni verifica Assured Recovery. I dati del server di replica verranno ripristinati nel preciso stato in cui si trovavano prima che il test iniziasse a utilizzare la tecnologia di ripristino. Quindi, verrà ripreso il processo di replica.

Esecuzione della verifica Assured Recovery in modalità non pianificata

Quando si imposta l'esecuzione della verifica Assured Recovery in una modalità pianificata, il test verrà eseguito automaticamente su base pianificata. Dopo aver selezionato questa opzione, saranno disponibili le seguenti funzionalità di pianificazione flessibile:

- Test in giorni selezionati della settimana e in orari specifici di un ciclo di 24 ore.
- Sincronizzazione in periodi selezionati (ad esempio, una volta ogni 36 ore) in un ciclo di 7 giorni.
- Esclusione di date specifiche.

È possibile impostare la verifica Assured Recovery durante la creazione dello scenario o in un secondo momento.

Nota: è possibile definire solo un'attività pianificata per scenario. Se si tenta di configurare la verifica Assured Recovery quando è già stata configurata un'operazione di sospensione pianificata, verrà visualizzato il seguente messaggio: **È possibile impostare solo un'attività pianificata per scenario. La sospensione è già impostata su ATTIVO per l'host [nome_server_di_replica]. DISATTIVARE l'opzione ora?** Per impostare l'opzione di pianificazione sulla verifica Assured Recovery, fare clic su Sì.

Per pianificare la verifica Assured Recovery, procedere come segue:

1. Dal riquadro Scenario, selezionare il server di replica che si desidera sottoporre alla verifica.

   Nel riquadro Struttura a sinistra, selezionare la scheda Proprietà High Availability.

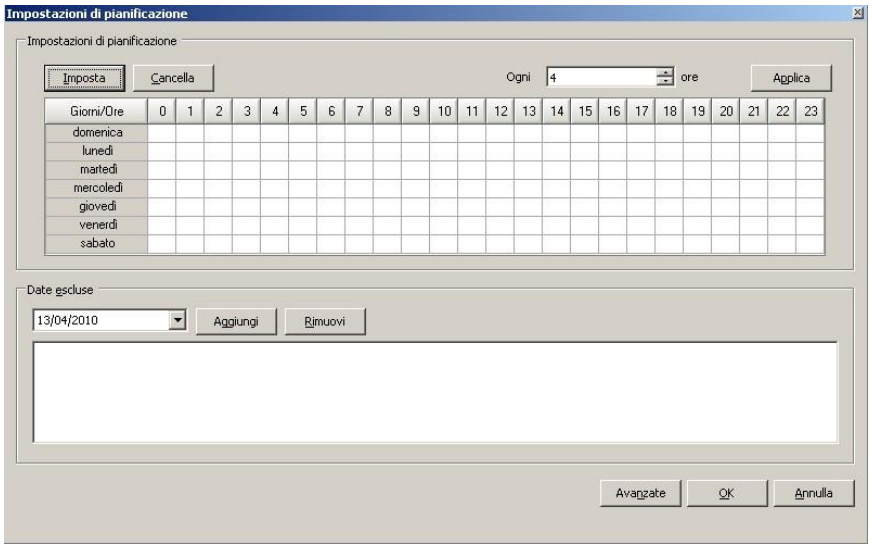
   Viene visualizzato un elenco delle proprietà del server di replica.

2. Se lo scenario è in esecuzione, fare clic sul pulsante Interrompi sulla barra degli strumenti standard.

   Lo scenario viene interrotto.

3. Nell'elenco Proprietà di replica, aprire il gruppo Attività pianificate. Quindi, nel gruppo Verifica di integrità di replica per Assured Recovery, selezionare la proprietà Utilità di pianificazione e fare clic sul valore Non impostato.

   Viene visualizzata la finestra di dialogo Ore Assured Recovery.



La finestra di dialogo Ore Assured Recovery è simile alla finestra di dialogo Impostazioni di pianificazione, utilizzata per pianificare la sincronizzazione automatica. Per informazioni sull'impostazione di una pianificazione, consultare la sezione Pianificazione della sincronizzazione (a pagina 211).

4. Pianificare l'esecuzione automatica della verifica Assured Recovery nella finestra di dialogo Ore Assured Recovery e fare clic su OK per salvare la pianificazione e chiudere la finestra.
5. Per attivare l'utilità di pianificazione, fare clic sul pulsante Salva nella barra degli strumenti standard e avviare lo scenario Assured Recovery.

   Il server di replica selezionato per la verifica verrà controllato periodicamente in base al piano impostato.

Esecuzione della verifica Assured Recovery in modalità non pianificata

In modalità non pianificata è possibile eseguire la verifica Assured Recovery automaticamente o manualmente. Quando si utilizza il metodo automatico, è possibile avviare la verifica Assured Recovery semplicemente premendo un pulsante. Quindi, Arcserve RHA eseguirà automaticamente tutti i passaggi della verifica, in base alle impostazioni di configurazione Assured Recovery. Una volta completata la verifica, verrà ripreso il normale processo di replica. Esiste un'unica differenza tra questo metodo e una verifica Assured Recovery pianificata. Nella modalità automatica non pianificata, è possibile avviare la verifica ogni volta che lo si desidera, senza utilizzare l'Utilità di Pianificazione.

Anche quando si utilizza il metodo manuale,è possibile avviare la verifica Assured Recovery semplicemente premendo un pulsante. Ad ogni modo, a differenza del metodo automatico, Arcserve RHA sospenderà il test dopo il primo passaggio standard, avviando il servizio database. Ciò si verificherà anche quando tutti i passaggi standard sono stati configurati come automatici.

Nota: se la proprietà Avvia database è impostata su Non attivo e non sono presenti script definiti dall'utente che la sostituiscano, l'unica operazione che Arcserve RHA potrà eseguire è la sospensione dell'applicazione delle modifiche al server di replica in preparazione della verifica Assured Recovery manuale.

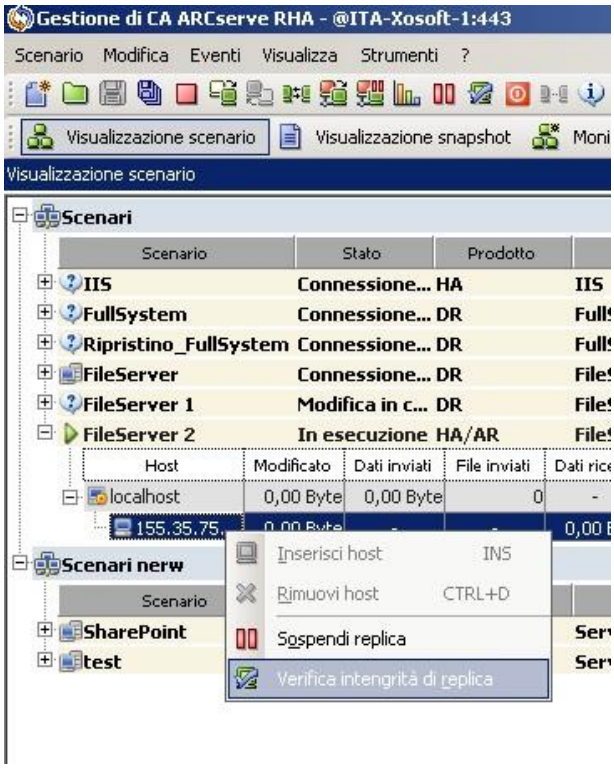
Quando la replica sarà stata sospesa, sarà possibile eseguire test o azioni direttamente sul server di replica, senza dover risincronizzare in seguito il server master e di replica. È possibile utilizzare questa opzione per effettuare il test manuale di applicazioni o dati sul server di replica oppure per eseguire attività sul server di replica invece che sul server master; ad esempio, la generazione di rapporti, allo scopo di ridurre il carico di lavoro del server master.

Al termine del test o dell'operazione manuale, sarà necessario arrestare manualmente la sospensione della verifica Assured Recovery. Anche in questo caso, è possibile farlo premendo semplicemente un pulsante. Se durante la verifica Assured Recovery sono stati configurati altri passaggi e azioni, quali l'arresto dei servizi di database, questi verranno eseguiti dopo aver fatto clic sul pulsante di arresto del test e prima che il test sia dichiarato come completato. Quando il test è considerato come terminato, la replica riprenderà automaticamente.

Esecuzione automatica della verifica Assured Recovery

Per eseguire automaticamente la verifica Assured Recovery, procedere come segue:

1. In Gestione, verificare che lo scenario Assured Recovery sia in esecuzione.
2. Per avviare la verifica Assured Recovery dal riquadro Scenario selezionare il server di replica che si desidera verificare. Quindi, fare clic sul pulsante Verifica integrità di replica nella barra degli strumenti standard oppure fare clic con il pulsante destro del mouse sul server di replica e scegliere Verifica integrità di replica dal menu di scelta rapida.



Viene visualizzata la finestra di dialogo Verifica di integrità di replica per Assured Recovery.

In questa finestra di dialogo è visualizzata la configurazione impostata per la verifica Assured Recovery.

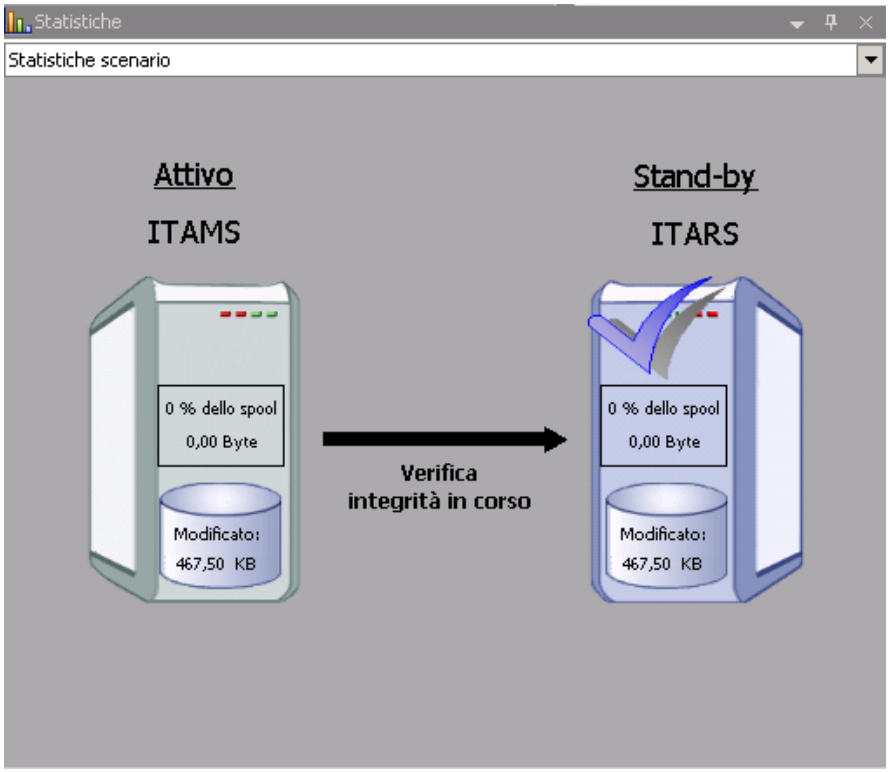
3. Per avviare automaticamente la verifica Assured Recovery utilizzando la configurazione esistente, fare clic su OK.

   Note:

   - Per modificare la configurazione del test prima di eseguirlo, fare clic su Annulla, e consultare la sezione Impostazione delle proprietà Assured Recovery.
   - Per eseguire manualmente la verifica Assured Recovery, selezionare la casella di controllo Verifica manuale, fare clic su OK e consultare la sezione Esecuzione manuale della verifica Assured Recovery (a pagina 325).

4. Dopo aver avviato la verifica, la finestra di dialogo Verifica di integrità di replica per Assured Recovery verrà chiusa. Quindi, prima dell'esecuzione della verifica, Arcserve RHA verificherà che non siano in corso operazioni di sincronizzazione, verifiche Assured Recovery o attività di sospensione della replica sugli host facenti parte dello scenario corrente.

5. Al termine della fase di verifica, viene avviata la verifica Assured Recovery.



I passaggi della verifica sono visualizzati come messaggi nel riquadro Eventi.

6. Al termine della verifica, il server di replica verrà ripristinato al preciso stato in cui si trovava quando la replica è stata sospesa. Ciò è possibile grazie alla sottostante tecnologia di ripristino. Quindi, le modifiche accumulate nello spool verranno applicate e la replica verrà ripresa, continuando normalmente.
7. Per impostazione predefinita, in seguito all'esecuzione di una verifica Assured Recovery, verrà generato un rapporto Assured Recovery.

   Note:

   - Se il rapporto non viene generato, nell'elenco delle proprietà del server di replica del gruppo Rapporti, verificare il valore della proprietà Genera rapporto Assured Recovery.
   - Per visualizzare il rapporto, consultare la sezione Visualizzazione di un rapporto (a pagina 167).

   Tutte le attività che sono state eseguite durante la verifica verranno elencate nel rapporto Assured Recovery, assieme all'ora e allo stato di attivazione.

Esecuzione manuale della verifica Assured Recovery

Invece di utilizzare l'Utilità di pianificazione, è possibile eseguire manualmente la verifica Assured Recovery.

Per eseguire manualmente la verifica Assured Recovery, procedere come segue:

1. In Gestione, verificare che lo scenario Assured Recovery sia in esecuzione.
2. Per avviare la verifica Assured Recovery dal riquadro Scenario selezionare il server di replica che si desidera verificare. Quindi, fare clic sul pulsante Verifica integrità di replica nella barra degli strumenti standard oppure fare clic con il pulsante destro del mouse sul server di replica e scegliere Verifica integrità di replica dal menu popup.

   Viene visualizzata la finestra di dialogo Verifica di integrità di replica per Assured Recovery.

   In questa finestra di dialogo è visualizzata la configurazione impostata per la verifica Assured Recovery.
3. Per avviare manualmente la verifica Assured Recovery utilizzando la configurazione esistente, selezionare la casella di controllo Verifica manuale. Dopo aver selezionato questa casella di controllo, la finestra di dialogo rifletterà solo le azioni che verranno eseguite in modalità manuale.

   Note:

   - Per modificare la configurazione della verifica prima di eseguirla, fare clic su Annulla e consultare la sezione Impostazione delle proprietà Assured Recovery.
   - Per eseguire automaticamente il test Assured Recovery, deselezionare la casella di controllo Verifica manuale, fare clic su OK e consultare la sezione Esecuzione automatica della verifica Assured Recovery (a pagina 323).

4. Fare clic su OK per chiudere la finestra di dialogo e avviare la verifica manuale.
   - Se la proprietà Avvia database è attivata oppure se è stato impostato uno script definito dall'utente per sostituirlo, tali azioni verranno eseguite e quindi la verifica verrà sospesa.
   - Se in questo passaggio non è stata impostata alcuna azione, la replica e la verifica verranno sospesi.
5. Da questo punto in poi, l'unica azione automatica eseguita da Arcserve RHA, a meno che non vengano configurate altre azioni come automatiche, è la sospensione degli aggiornamenti sul server di replica.
6. Una volta sospesa la replica, verrà visualizzato il seguente messaggio nel riquadro Eventi: Replica is ready for Manual Integrity Testing (Il server di replica è pronto per la verifica di integrità manuale).

   È ora possibile eseguire qualsiasi test desiderato direttamente sull'host di replica, incluse le modifiche del database. Si osservi che, a causa del processo di ripristino, tali modifiche non verranno salvate al termine della verifica Assured Recovery.

   Importante: Non riavviare il server di replica testato in questa fase; in caso contrario, tutte le modifiche accumulate nello spool andrebbero perdute.
7. Dopo aver terminato il test dell'host di replica, fare clic nuovamente sul pulsante Verifica integrità di replica per riprendere la replica.

   Importante: se non si fa clic sul pulsante Verifica integrità di replica una seconda volta al termine del test, le modifiche continueranno ad essere inserite nello spool dell'host di replica. Alla fine, si verifica l'overflow dello spool sull'host di replica e lo scenario viene interrotto.

   Viene visualizzato un messaggio di conferma.
8. Fare clic su **Sì** per interrompere la verifica Assured Recovery. Se durante la verifica Assured Recovery sono stati configurati altri passaggi e azioni, quali l'arresto dei servizi di database, questi verranno eseguiti prima che il test sia dichiarato come completato. Quando la verifica è considerata come terminata, la replica riprenderà automaticamente.
9. Al termine della verifica, il server di replica verrà ripristinato al preciso stato in cui si trovava quando la replica è stata sospesa. Quindi, le modifiche accumulate nello spool verranno applicate e la replica verrà ripresa, continuando normalmente.
10. Per impostazione predefinita, in seguito all'esecuzione di una verifica Assured Recovery, verrà generato un rapporto Assured Recovery.

Capitolo 13: Utilizzo di snapshot VSS

Arcserve RHA consente di usare facilmente il servizio Volume Shadow Copy Service (VSS) di Microsoft per creare, visualizzare e gestire snapshot VSS dei dati di replica.

Importante: è possibile utilizzare VSS solo su Windows Server 2003 e versioni successive (non su versioni precedenti).

È possibile impostare la creazione automatica delle snapshot VSS in associazione con due operazioni: durante la sospensione della replica e dopo il corretto completamento della verifica Assured Recovery. In aggiunta, se Arcserve RHA è integrato con Arcserve, verrà creata automaticamente una snapshot VSS per ogni backup di Arcserve. Tutte queste snapshot vengono visualizzate nella finestra Gestione snapshot di Arcserve RHA, che consente di monitorare e gestire le snapshot.

Questa sezione contiene i seguenti argomenti:

Creazione automatica di snapshot VSS (a pagina 327)
Visualizzazione e gestione delle snapshot (a pagina 331)

Creazione automatica di snapshot VSS

Per impostazione predefinita, Arcserve RHA non crea automaticamente snapshot VSS. Per attivare questa opzione, sarà necessario impostare su Attivato la proprietà **Crea copia replicata (VSS)** del server di replica richiesto. Questa proprietà è associata a due operazioni: sospensione della replica e verifica Assured Recovery. Dal momento che non è possibile impostare entrambe le operazioni su una modalità pianificata per lo stesso server di replica, è necessario configurare la proprietà **Crea copia replicata (VSS)** in considerazione di una di queste operazioni.

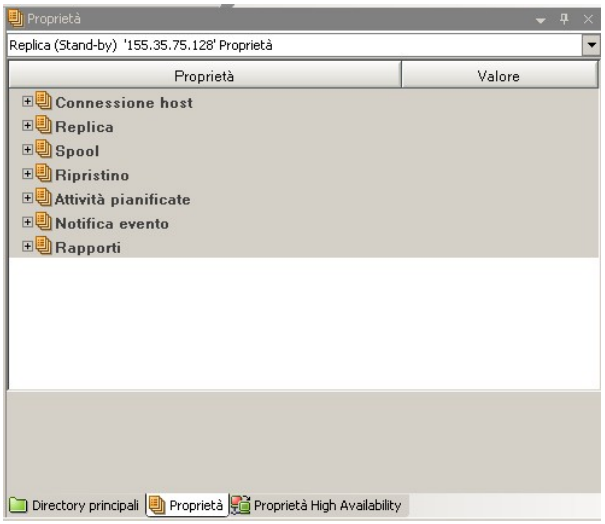
Nota: la sospensione manuale non comporta la creazione di snapshot VSS. Le snapshot VSS verranno automaticamente create solo se associate alla sospensione pianificata.

Impostazione della creazione di snapshot

Per impostare la creazione di una snapshot, procedere come segue:

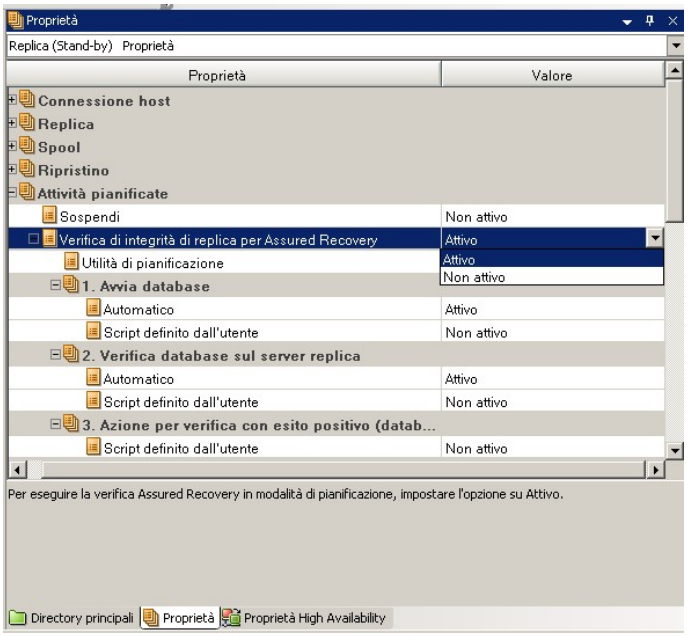
1. Dal riquadro Scenario, selezionare il server di replica per il quale si desidera creare snapshot VSS.
2. Nel riquadro Struttura a sinistra, selezionare la scheda Proprietà High Availability.

   Viene visualizzato l'elenco Proprietà di replica.



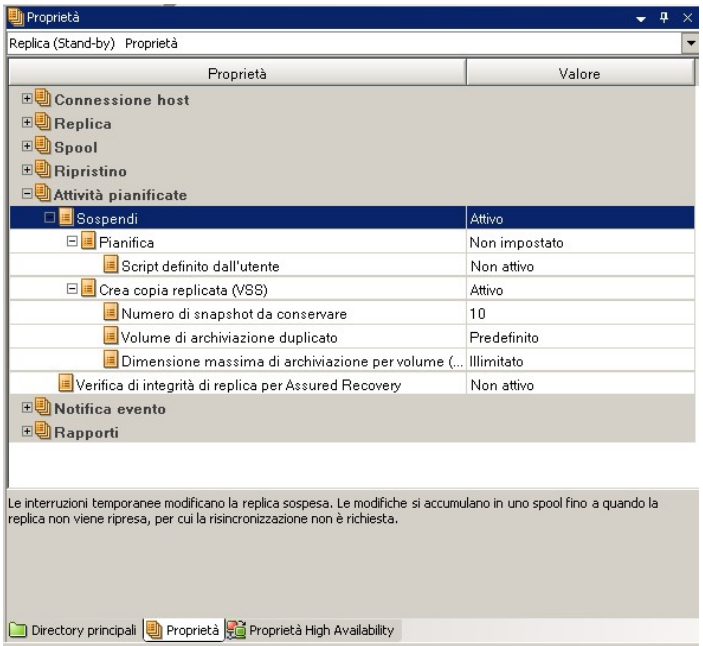
3. Se lo scenario è in esecuzione, fare clic sul pulsante **Interrompi** sulla barra degli strumenti. Lo scenario viene interrotto.

4. Nell'elenco Proprietà di replica, aprire il gruppo **Attività pianificate** per visualizzare le proprietà **Sospendi** e **Verifica di integrità di replica per Assured Recovery**.



5. Impostare il valore su Attivo per la proprietà **Sospendi** o **Verifica di integrità di replica per Assured Recovery**.

   Viene visualizzata la proprietà **Crea copia replicata (VSS)** assieme alle proprietà correlate.



È possibile impostare l'opzione VSS nella sezione Attività pianificate.

Per modificare le proprietà di Crea copia replicata (VSS), accedere a Proprietà di gestione snapshot del volume.

Note:

- Se si imposta la proprietà **Verifica di integrità di replica per Assured Recovery** su Attivo, la proprietà **Crea copia replicata (VSS)** appare nel gruppo **Azione in caso di esito positivo della verifica (database non in linea)**.
- Per associare la creazione di snapshot VSS alla proprietà **Sospendi**, è necessario pianificare la sospensione. La sospensione manuale non comporta la creazione di snapshot VSS.

6. Per attivare la creazione automatica delle snapshot, impostare il valore della proprietà **Crea copia replicata (VSS)** su Attivato.
7. Impostare le altre proprietà VSS, in base alle informazioni fornite nella sezione Nozioni fondamentali sulle proprietà delle snapshot VSS (a pagina 331).
8. Fare clic sul pulsante **Salva** nella barra degli strumenti per salvare e applicare le proprie modifiche, quindi avviare lo scenario.

A questo punto, dopo una verifica di Assured Recovery o durante la sospensione, verrà creata automaticamente una snapshot VSS. La creazione della snapshot viene indicata nel riquadro Evento.

Dopo aver creato la snapshot, è possibile visualizzarla e gestirla nella finestra Gestione snapshot.

Nozioni fondamentali sulle proprietà delle snapshot VSS

In questa sezione vengono elencate le proprietà delle snapshot VSS, i valori corrispondenti e una spiegazione per ciascuna proprietà.

Crea copia replicata (VSS)

Per creare snapshot VSS in modo automatico durante la sospensione della replica o dopo una verifica Assured Recovery completata correttamente, impostare questa opzione su Attivato.

Numero preferito di snapshot da conservare

Immettere il numero di snapshot che si preferisce salvare e monitorare. Una volta raggiunto questo numero, le snapshot più obsolete verranno sostituite con quelle più recenti. Tuttavia, se la snapshot più vecchia è montata o bloccata per il backup, non verrà eliminata. Quindi, la nuova snapshot verrà aggiunta all'elenco di snapshot anche se è stato superato il numero impostato. Altre ragioni VSS interne potrebbero comportare un numero di snapshot salvate superiore a quello specificato. Il numero predefinito è di 10 snapshot.

Volume di archiviazione copie replicate universale

Specificare il volume in cui verranno archiviate le snapshot. Si osservi che non è possibile impostare separatamente questa proprietà per ogni scenario. La posizione di archiviazione della prima snapshot VSS che viene creata nel sistema si applica a tutte le snapshot successive.

Dimensione max archiviazione per volume

Immettere la capacità massima di archiviazione per volume utilizzata dalle snapshot (MB).

Visualizzazione e gestione delle snapshot

Arcserve RHA dispone di una finestra specifica per la gestione delle snapshot VSS.

Visualizzazione di snapshot

Per aprire la finestra Gestione snapshot, procedere come segue:

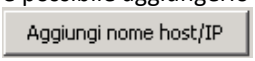
- Nella Gestione, fare clic sul pulsante **Visualizzazione snapshot**

nella barra degli strumenti di visualizzazione.

  Viene visualizzata la finestra **Gestione snapshot**.

  In questa finestra, vengono visualizzate le snapshot VSS create per ogni server di replica esistente, secondo il server di replica selezionato.

È possibile modificare il server di replica di cui si visualizzano le snapshot utilizzando l'elenco a discesa **Selezionare host di replica**. Gli host di replica visualizzati nell'elenco sono quelli partecipanti agli scenari esistenti.

Se un server di replica caratterizzato da snapshot partecipava a uno scenario che è stato rimosso dalla Gestione, non verrà visualizzato nell'elenco. Per visualizzare snapshot di un server di replica non più presente in elenco, è possibile aggiungerlo manualmente mediante il pulsante **Aggiungi nome host/IP** 

.

Per ogni snapshot vengono fornite le seguenti informazioni.

- **Nome scenario**: lo scenario in cui è stata creata la snapshot.
- **Guida di snapshot**: ID univoco che identifica la snapshot.
- **Creato**: data e ora della creazione della snapshot.
- **Autore**: il tipo di operazione associato alla creazione della snapshot. Sono disponibili due tipi: Suspend (Sospensione) e Assured Recovery.
- **È esposto**: indica se la snapshot è stata esposta ("Vero") o no ("Falso").
- **Esponi percorso**: la posizione in cui la snapshot è stata esposta.
- **Percorso di origine**: il volume/la directory dal quale è stata acquisita la snapshot.
- **Percorso di archiviazione**: posizione in cui è stata archiviata la snapshot.
- **Bloccato per backup**: questa colonna si riferisce alle snapshot acquisite come parte del backup di Arcserve. Se il backup non è ancora completo, non sarà possibile gestire la snapshot e il valore visualizzato sarà "Vero". Se il backup è completo oppure se la snapshot non è associata a Arcserve, il valore è "False".

Dopo aver visualizzato le snapshot è possibile passare alla fase di gestione (a pagina 332).

Gestione delle snapshot

Per gestire le snapshot, procedere come segue:

- Nella finestra **Gestione snapshot**, selezionare la snapshot che si desidera gestire. Quindi, aprire il menu **Snapshot** e selezionare l'opzione desiderata oppure fare clic con il pulsante destro del mouse e selezionare l'opzione dal menu di scelta rapida.

  Le azioni disponibili sono:

  - **Monta in Cartella**: consente di montare una snapshot esposta in una cartella inutilizzata.
  - **Monta come lettera unità**: consente di montare una snapshot esposta su una lettera di unità inutilizzata.

- **Smonta**: consente di rilasciare una snapshot esposta senza perdere la snapshot stessa. La snapshot sarà comunque esposta, ma non utilizzerà un punto di montaggio.
- **Elimina**: consente di eliminare una snapshot. È possibile eliminare diverse snapshot contemporaneamente utilizzando il tasto **CTRL**.
- **Aggiorna**: aggiorna l'elenco delle snapshot per visualizzare le snapshot più aggiornate.

Capitolo 14: Utilizzo della soluzione Content Distribution

In questa sezione vengono fornite istruzioni per la creazione, la gestione e l'utilizzo della soluzione di gestione contenuto.

Questa sezione contiene i seguenti argomenti:

Nozioni fondamentali sulla soluzione Content Distribution (a pagina 335)
Creazione scenario Distribuzione contenuto (CD) (a pagina 337)

Nozioni fondamentali sulla soluzione Content Distribution

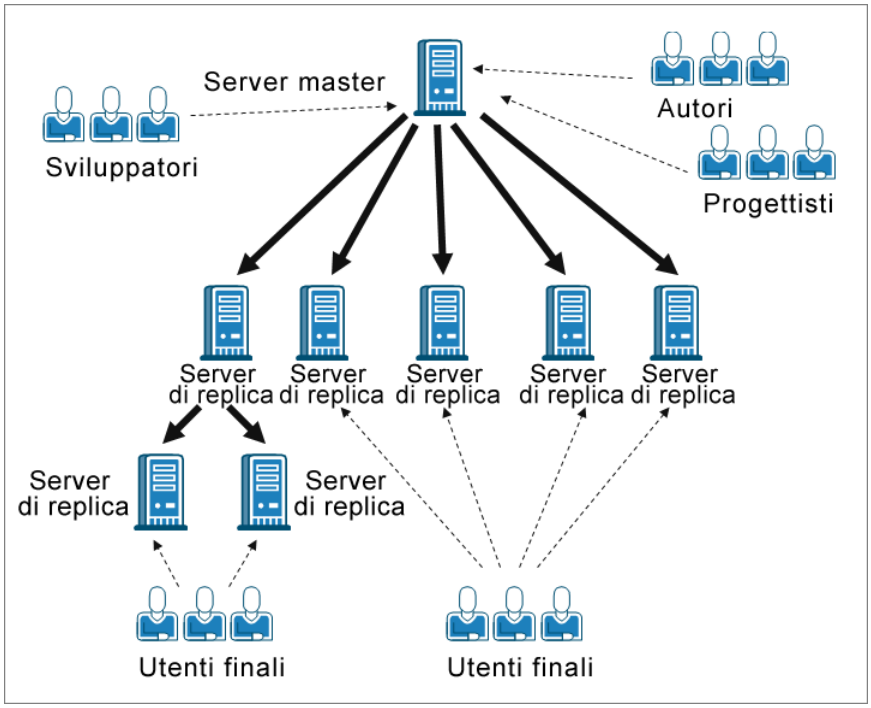
Importante: La soluzione Content Distribution richiede una licenza specifica.

La soluzione Content Distribution consente di diffondere e gestire in modo affidabile le informazioni in un ambiente altamente distribuito. In un ambiente IT, caratterizzato da un livello di distribuzione elevato, numerosi server contengono contenuto identico o simile che ricevono da un singolo repository e lo distribuiscono a molti utenti finali contemporaneamente. Un esempio di un ambiente distribuito di questo tipo è rappresentato dalle organizzazioni di grandi dimensioni, che hanno necessità di distribuire, sincronizzare e consolidare le informazioni aziendali tra utenti interni che risiedono in più sedi e filiali. Tali informazioni possono includere listini prezzi, criteri, materiali di vendita manuali e notizie. La soluzione Content distribution consente a dipendenti e rappresentanti che operano nel campo di disporre delle informazioni corrette nel momento opportuno.

Si tratta inoltre di uno strumento potente per la distribuzione del contenuto e la relativa pubblicazione sul Web in grado di servire gli utenti esterni. Grazie a portali e siti Web, è possibile distribuire ai clienti le informazioni memorizzate in file contenenti musica, filmati, documenti e notizie. Si tratta di un eccellente esempio di provider di servizi in grado di distribuire contenuto a decine, centinaia e migliaia di e-shop del mondo.

In uno scenario Replication o HA normale, generalmente il master è il server attivo o di produzione, mentre gli host di replica costituiscono principalmente un'area di archiviazione per i dati replicati o i server in stand-by. A differenza di questa struttura dei ruoli, in uno scenario CD, gli host di replica sono solitamente gli host attivi, che forniscono direttamente informazioni agli utenti finali, mentre gli host master agiscono solo come provider iniziali dei dati aggiornati. Il contenuto viene gestito in un singolo repository sull'host master, mentre le modifiche agli host di replica vengono distribuite immediatamente o su base una pianificata. Quando si implementa la soluzione CD in un'organizzazione di grandi dimensioni, più scenari CD possono utilizzare le stesse directory oppure directory principali sovrapposte, applicare opzioni di filtro differenti e replicare i dati in un gruppo di host di replica diverso.

La soluzione CD è progettata per scenari uno a molti, ovvero scenari che includono un singolo host master e un numero elevato di host di replica. Scenari di questo tipo possono consentire la replica di numerosi file oppure utilizzare un numero ridotto di file di grandi dimensioni. In scenari simili, numerosi host di replica sono organizzati con una disposizione orizzontale, ossia come appartenenti allo stesso livello e non inclusi in un ordine gerarchico secondo relazioni padre-figlio.



Se in uno scenario normale, contenente diversi host di replica sullo stesso livello, è necessario risincronizzare più host di replica in seguito a un riavvio o a errori di connessione, la risincronizzazione deve essere estesa anche a tutti gli altri host. Tuttavia questa procedura può causare problemi di prestazioni in una condizione in cui sono presenti centinaia o migliaia di host di replica. Quindi se in uno scenario CD, è necessario risincronizzare più host di replica, vengono risincronizzati solo gli host che effettivamente richiedono questa operazione.

Un'altra caratteristica degli scenari normali che può causare problemi in un ambiente distribuito, è la modalità di replica online. In una modalità di replica online normale, le modifiche apportate agli host master vengono immediatamente trasferite all'host di replica e sovrascrivono i dati in essi presenti. Questo processo è importante per conservare i dati più aggiornati sul server di replica, tuttavia quando gli utenti utilizzano direttamente i dati memorizzati nel server di replica, potrebbero andare sperimentare interruzioni causate dagli aggiornamenti continui. Per risolvere il problema, uno scenario CD può essere eseguito in una modalità di replica speciale, denominata **Alla chiusura del file,** disponibile solo per gli scenari CD.

In modalità **Alla chiusura del file**, tutti i dati accumulati sull'host master vengono trasferiti all'host di replica, tuttavia non sovrascrivono immediatamente i dati di replica esistenti. Al contrario, i dati modificati e trasferiti all'host di replica vengono salvati come copia temporanea del file originale e memorizzati in una directory nascosta. Una volta chiuso il file originale sull'host master, la copia temporanea sull'host di replica viene rinominata. Quando la copia sull'host di replica riceve il nome del file originale, sostituisce il file precedente memorizzato sull'host di replica, mantenendo i dati aggiornati su tale server. Questo metodo consente di utilizzare un processo di aggiornamento che non interrompe il lavoro dell'utente. Se, tuttavia, la modalità **Alla chiusura del file** non soddisfa i requisiti del proprio ambiente, è anche possibile utilizzare la modalità di replica online o pianificata per la propria soluzione CD.

Creazione scenario Distribuzione contenuto (CD)

La creazione di uno scenario CD è un processo analogo alla creazione di uno scenario di replica per i server applicazioni e di database. In entrambi è possibile utilizzare creazione guidata dello scenario. L'unica principale differenza tra i due processi è che quando si seleziona la modalità di replica di uno scenario CD, è disponibile una modalità di replica aggiuntiva. Questa modalità di replica, denominata **Alla chiusura del file**, è disponibile solo ai fini della distribuzione del contenuto.

Nota: in questa sezione viene illustrata la configurazione di uno scenario generico di distribuzione del contenuto del file server. Per istruzioni più dettagliate sugli scenari personalizzati per applicazioni specifiche, consultare la Guida operativa appropriata.

Per creare uno scenario di distribuzione del contenuto, procedere come segue:

1. Aprire la Gestione Arcserve RHA. Quindi, dal menu **Scenario** scegliere l'opzione **Nuovo**, oppure fare clic sul pulsante **Nuovo** sulla barra degli strumenti standard.

   Viene visualizzata la **Creazione guidata scenario**.

2. Selezionare le opzioni dello scenario necessarie, come riportate di seguito:
   - Selezionare il pulsante di opzione **Crea nuovo scenario**.
   - Dall'elenco a discesa **Gruppo** selezionare il gruppo a cui assegnare il nuovo scenario. In alternativa, immettere il nome di un nuovo gruppo.

3. Fare clic su **Avanti**. Viene visualizzata la schermata **Selezionare server e tipo di prodotto**.

   Viene presentato un elenco di applicazioni e tipi di scenari disponibili.

   Nota: l'elenco di applicazioni disponibili dipende dalle licenze applicate**.**

4. Selezionare le opzioni dello scenario necessarie, come riportate di seguito:

   - Dall'elenco **Seleziona tipo server**, selezionare il tipo di server per il quale si desidera creare lo scenario.
   - Dalle opzioni **Seleziona tipo prodotto**, selezionare **Scenario distribuzione contenuto**.

   Nota: le opzioni **Attività su replica** non sono disponibili per la soluzione CD.

5. Fare clic su **Avanti**. Viene visualizzata la schermata **Host master e replica**.

6. Immettere le seguenti informazioni:

   - Nella casella **Nome scenario** è possibile confermare il nome predefinito oppure immetterne uno nuovo. Quando si immette un nome, scegliere un nome univoco dal momento che non sarà possibile utilizzare lo stesso nome per più scenari.
   - Nelle caselle **Nome host/IP master** e **Nome host/IP di replica**, immettere il nome host o l'indirizzo IP dei server master (origine) e replica (destinazione) oppure utilizzare i pulsanti **Sfoglia** per trovarli.
   - Nelle caselle **Porta**, accettare il numero di porta predefinito (25000) o immettere i nuovi numeri di porta per il master e la replica.

   Nota: se si desidera includere più server di replica nello scenario, immettere qui i dettagli del primo server di replica o di quello più a monte. Una volta completata la creazione dello scenario, immettere manualmente gli altri server di replica, come descritto nella sezione Aggiunta di server di replica supplementari (a pagina 173).

7. [Facoltativo] Selezionare la casella di controllo **Modalità valutazione** se si desidera raccogliere dati statistici accurati sull'utilizzo della larghezza di banda e sui punti di riferimento del rapporto di compressione necessari per la replica, senza effettivamente replicare i dati. Se si seleziona questa opzione, la replica non verrà eseguita, ma al termine del processo di valutazione verrà fornito un rapporto.

8. [Facoltativo] Selezionare la casella di controllo **Verifica Modulo Arcserve RHA sugli host** se si desidera che il sistema verifichi che i moduli siano installati e in esecuzione sugli host master e di replica specificati in questa pagina. Se i moduli non sono stati installati sugli host selezionati, è possibile utilizzare questa opzione per installare in remoto i moduli su uno o su entrambi gli host. Per ulteriori informazioni sulla pagina di **verifica host**, si rimanda alla sezione Creazione di uno scenario (a pagina 47).

9. Dopo aver selezionato le opzioni desiderate, fare clic su **Avanti**. Viene visualizzata la schermata **Directory principali master**.

   Arcserve RHA visualizza le directory e i file che si trovano sul server master. Si tratta delle directory e dei file di cui possibile replicare, proteggere e distribuire i dati Arcserve RHA raggruppa automaticamente i dati con un percorso comune in un'unica directory.

10. Scegliere le directory e i file che si desidera replicare dai server master e di replica selezionando le relative caselle di controllo. Per escludere cartelle e file dalla replica, deselezionare la relativa casella di controllo.

    Note:

    - Per ulteriori informazioni sulle modalità di selezione e filtro delle directory principali, si rimanda alla sezione Creazione di uno scenario di replica (a pagina 47).
    - Al termine della creazione dello scenario mediante la procedura guidata, è anche possibile selezionare chiavi di registro per la sincronizzazione, come descritto nella sezione Sincronizzazione chiavi di registro (a pagina 184).

11. Dopo aver definito i dati da replicare, fare clic su **Avanti**.

    Viene visualizzata la schermata **Directory principali di replica**.

    In questa schermata, selezionare le directory sul server di replica in cui saranno memorizzati i dati replicati.

    Importante: La creazione guidata dello scenario configura automaticamente le directory principali del server di replica in modo analogo alle directory principali del server master. Se si desidera mantenere questa configurazione, assicurarsi che la lettera dell'unità del server di replica sia la stessa di quella del server master e che le directory selezionate sul server di replica non contengano dati che si desidera salvare. È possibile modificare la configurazione predefinita successivamente, come descritto in Selezione di directory principali di replica (a pagina 191).

12. Per modificare le directory principali del server di replica, fare doppio clic sul percorso delle directory specificate. Viene visualizzata la finestra di dialogo **Sfoglia e seleziona directory di replica**.

13. Selezionare la directory sul server di replica in cui saranno memorizzati i dati replicati, quindi fare clic su **OK**.

    Viene visualizzata la schermata **Directory principali di replica**.

    Nota: è possibile modificare manualmente la directory selezionata per l'archiviazione dei dati replicati facendo clic sul nome della directory selezionata e immettendone una nuova. Se il nome immesso per la directory è inesistente sul server di replica, Arcserve RHA lo creerà automaticamente.

14. Dopo aver definito la posizione di archiviazione dei dati replicati, fare clic su **Avanti**.

    Viene visualizzata la schermata **Proprietà scenario**.

    Nella schermata **Proprietà scenario** è possibile configurare le proprietà dello scenario che influiscono sull'intero scenario. In genere, i valori predefiniti sono sufficienti.

    Per configurare le proprietà dello scenario in questa fase, consultare la sezione Nozioni fondamentali sulle proprietà dello scenario (a pagina 202). Per configurare le proprietà dello scenario in una fase successiva, consultare la sezione Configurazione delle proprietà dello scenario (a pagina 201).

15. Nella schermata **Proprietà scenario** è possibile impostare la modalità di replica dello scenario. Oltre alle due modalità di replica standard, **In linea** e **Pianificazione**, Arcserve RHA offre una modalità aggiuntiva appositamente progettata per lo scenario di distribuzione contenuto: la modalità di replica **Alla chiusura del file** . La modalità **Alla chiusura del file** è simile alla modalità di replica **Online** con una differenza: mentre le modifiche dei dati in modalità **Online** trasferite dal server master al server di replica sovrascrivono immediatamente i dati di replica esistenti, in modalità **Alla chiusura del file** le modifiche apportate ai singoli file vengono visualizzate nel server di replica solo dopo che il file originale sul server master è stato chiuso. In questo modo, se gli utenti stanno lavorando direttamente sui dati memorizzati nel server di replica, la loro attività non verrà interrotta da aggiornamenti continui.

    Nota: la modalità di replica predefinita è **Online**.

Per impostare la modalità d replica, aprire il gruppo **Replica** e selezionare la proprietà **Modalità**. Quindi, selezionare la modalità di replica richiesta dall'elenco a discesa.

16. Dopo aver impostato le proprietà dello scenario, fare clic su **Avanti**. Viene visualizzata la schermata **Proprietà di master e replica**.

    Nella schermata **Proprietà di master e replica** è possibile configurare le proprietà correlate all'host master o di replica. In genere, i valori predefiniti sono sufficienti.

    Per configurare le proprietà dei server master e di replica in questa fase, consultare la sezione Impostazione delle proprietà del server master e di replica (a pagina 215). Per configurare le proprietà dei server master e di replica in una fase successiva, consultare la sezione Configurazione delle proprietà del server master e di replica (a pagina 216).

    Nota: è possibile modificare tutte le impostazioni in questo riquadro dopo aver creato lo scenario. Tuttavia, prima di modificare le proprietà di spool (che è possibile configurare in questo passaggio), consultare la sezione Spool (a pagina 220) per i dettagli di configurazione.

17. Dopo aver impostato le Proprietà di master e replica, fare clic su **Avanti**.

    Arcserve RHA verifica la validità del nuovo scenario e controlla vari parametri tra i server master e di replica per garantire la corretta esecuzione dei processi di replica, distribuzione e ripristino dei dati. Una volta completata la verifica, viene visualizzata la schermata **Verifica scenario**.

    Nota: sebbene Arcserve RHA consenta all'utente di procedere nonostante vengano visualizzati avvisi, si sconsiglia di farlo. Per assicurare un corretto funzionamento dell'applicazione, risolvere le situazioni che generano messaggi di avviso prima di continuare.

18. Dopo aver eseguito la verifica dello scenario, fare clic su **Avanti**.

    Viene visualizzata la schermata **Esecuzione scenario**.

19. Dopo aver eseguito la verifica dello scenario, viene richiesto di eseguirlo. L'esecuzione dello scenario consente di avviare il processo di sincronizzazione dei dati.

    - Per aggiungere ulteriori host di replica ed eseguirli in un secondo momento, selezionare **Fine**.

      Nota: Arcserve RHA fornisce due metodi per aggiungere host di replica allo scenario:

      - Mediante la Gestione Arcserve RHA, aggiungendo manualmente ogni host allo scenario, come descritto nella sezione Aggiunta di server di replica supplementari (a pagina 173).
      - Mediante PowerShell per Arcserve RHA, utilizzando i comandi **Add-Replica (Aggiungi replica)** e **Add-Replicas (Aggiungi repliche)**. Per ulteriori informazioni sull'utilizzo dei comandi PowerShell per Arcserve RHA, consultare la *Guida per PowerShell di Arcserve RHA.*

    - Per eseguire il processo immediatamente, selezionare **Esegui ora**.

      Viene avviato il processo di sincronizzazione.

20. Il processo di sincronizzazione potrebbe richiedere tempo, a seconda della dimensione del database e della larghezza di banda di rete esistente tra il server master e di replica. Quando la sincronizzazione è completata, nel riquadro Evento viene visualizzato il seguente messaggio: **Tutte le modifiche avvenute durante il periodo di sincronizzazione sono state replicate**. A questo punto, la replica in tempo reale è operativa e la soluzione Content Distribution sarà installata e attiva.

    Nota: se lo scenario include più host di replica, la scheda **Statistiche scenario** non visualizza una panoramica grafica dello stato dello scenario, bensì le relative statistiche organizzate in tabelle.

21. Per impostazione predefinita, una volta eseguita una sincronizzazione, viene generato un rapporto di sincronizzazione. Per ciascuno host di replica che partecipa allo scenario, viene generato un rapporto di sincronizzazione. Per ulteriori informazioni sull'apertura dei rapporti, consultare la sezione Visualizzazione di un rapporto (a pagina 167).

Capitolo 15: Gestione utenti

Arcserve RHA consente di gestire i diritti di accesso di un utente mediante l'impostazione delle proprietà ACL del file dello scenario di distribuzione contenuto. ACL è un elenco di controllo di accesso, ovvero una lista di proprietà di protezione applicabili al file dello scenario.

Per disporre di questa opzione, è necessario acquistare una licenza specifica.

Nota: non è possibile gestire le proprietà ACL per gli scenari replication o High Availability.

Questa sezione contiene i seguenti argomenti:

Funzionamento della protezione delegata (a pagina 343)
Attività preliminari per la gestione utenti (a pagina 344)
Come gestire gli utenti (a pagina 346)

Funzionamento della protezione delegata

La protezione delegata consente di controllare i diritti di accesso di ciascun utente mediante l'impostazione delle proprietà dell'elenco di controllo di accesso file (ACL) dello scenario Content Distribution.

Il modello di autenticazione ACL è un tipo di autenticazione basato su ruoli di Arcserve RHA. Sono disponibili quattro ruoli predefiniti, ognuno dei quali include autorizzazioni a loro volta predefinite che stabiliscono le azioni che è possibile eseguire sullo scenario. I ruoli disponibili includono:

- Super utente
- Admin
- Controllo
- Solo visualizzazione

Il ruolo Utente con privilegi fornisce diritti di controllo completi su uno scenario, al contrario dei ruoli Admin, Controllo e Solo visualizzazione che concedono invece diritti limitati. Solo l'utente con privilegi può creare un nuovo scenario.

Per accedere a uno scenario un utente deve disporre di uno di questi quattro ruoli. Un utente a cui è stato assegnato il ruolo Utente con privilegi o Admin può assegnare utenti o gruppi a qualsiasi scenario e delegare diritti a utenti o gruppi. Quando un utente tenta di accedere a uno scenario mediante la Gestione Arcserve RHA o PowerShell per Arcserve RHA, il ruolo corrente viene controllato e, a seconda delle autorizzazioni di cui il ruolo dispone, l'operazione viene consentita o negata.

Considerazioni sui diritti di accesso

Prima di assegnare le autorizzazioni agli utenti, è necessario tenere conto dei seguenti elementi:

- Tutti gli utenti devono appartenere al dominio di Windows o essere utenti locali.
- Un utente con privilegi ha il diritto di creare un nuovo scenario.
- Un utente con privilegi o un utente Admin possono assegnare utenti o gruppi a qualsiasi scenario, nonché delegare diritti a utenti o gruppi mediante la Gestione Arcserve RHA.
- L'elenco di utenti o gruppi con i relativi diritti viene memorizzato nell'ACL NTFS standard applicato al file dello scenario.
- L'utente con privilegi può modificare il gruppo utente con privilegi. Tuttavia, una volta apportata la modifica, è necessario riassegnare i diritti a tutti gli scenari esistenti.
- Gli utenti possono impostare o modificare il gruppo utente con privilegi, il quale viene riportato in un registro crittografato. Tutti gli utenti con privilegi appartengono al gruppo.
- L'ACL è controllato indirettamente tramite il Servizio di controllo. Poiché al Servizio di controllo possono essere connesse più sessioni GUI, è necessaria l'identificazione di ciascun account utente.

Attività preliminari per la gestione utenti

È necessario eseguire le seguenti operazioni preliminari prima di impostare i diritti utente o di modificare i gruppi utenti.

Creazione di un gruppo di utenti

Quando si utilizzano le autorizzazioni ACL, prima di aprire la Pagina con informazioni introduttive e la Gestione, è necessario creare un gruppo locale. Definire il gruppo locale denominato Utenti Arcserve RHA sul computer del Servizio di controllo e su tutti i computer su cui è in esecuzione il Modulo Arcserve RHA e per i quali si desidera concedere agli utenti o ai gruppi le autorizzazioni per aggiungere e modificare gli host di replica oppure per accedere alle directory principali degli host.

Per creare un gruppo locale denominato Utenti Arcserve RHA, procedere come segue:

1. Sul computer in cui è in esecuzione il Servizio di controllo, fare clic sul pulsante Start, scegliere Impostazioni, Pannello di controllo, Strumenti di amministrazione, quindi Gestione computer.

   Viene visualizzata la finestra di dialogo Gestione computer.

2. Selezionare la cartella **Utenti e gruppi locali**, quindi aprire la sottocartella **Gruppi** .
3. Fare clic con il pulsante destro del mouse su **Gruppi** e selezionare **Nuovo gruppo**.

   Viene visualizzata la finestra di dialogo **Nuovo gruppo**.
4. Nella casella **Nome gruppo**, immettere Utenti Arcserve RHA.
5. Per aggiungere l'utente amministratore, fare clic sul pulsante **Aggiungi**.
6. Fare clic sul pulsante **Crea** per creare il nuovo gruppo locale, quindi sul pulsante **Chiudi** per chiudere la finestra di dialogo.

   Il nuovo gruppo viene aggiunto all'elenco Gruppi locali nel computer in cui è installato il Servizio di controllo.

Selezione del gruppo iniziale

Definire il gruppo locale denominato Utenti Arcserve RHA sul computer del Servizio di controllo e su tutti i computer su cui è in esecuzione il Modulo Arcserve RHA e per i quali si desidera concedere agli utenti o ai gruppi le autorizzazioni per aggiungere e modificare gli host di replica oppure per accedere alle directory principali degli host.

Quando si apre la Gestione per la prima volta, questa rileva se un gruppo utente con privilegi esiste già. Se non è stato definito alcun gruppo di questo tipo, viene visualizzata la finestra di dialogo**Imposta il gruppo utente con privilegi**.

La finestra di dialogo Imposta il gruppo utente con privilegi visualizza l'elenco di gruppi esistenti come gruppi locali nel computer in cui viene eseguito il Servizio di controllo. È necessario selezionare il gruppo che dovrà includere i membri che verranno definiti come utenti con privilegi. È possibile modificare questo gruppo in un secondo momento.

Impostazione di un gruppo utenti

Per impostare l'ambiente per l'utilizzo della protezione delegata basata su ACL, Arcserve RHA consente di utilizzare l'infrastruttura esistente per la creazione di una nuova rete e di un gruppo locale. Sono necessari quattro gruppi:

- Super utente
- Admin
- Controllo
- Visualizzazione

È possibile assegnare utenti a un gruppo specifico a seconda dei privilegi richiesti per il singolo utente. Per ulteriori informazioni sulle autorizzazioni utente, fare riferimento all'argomento Delega dei diritti (a pagina 346).

Nota: è possibile impostare gruppi aggiuntivi e designarli come Utente con privilegi, Admin, Controllo, Visualizzazione o utilizzare gruppi già esistenti nella rete.

Su ciascun computer facente parte dello scenario (Master, Replica e Servizio di controllo), creare un gruppo locale con il nome predefinito Utenti Arcserve RHA. Aggiungere i gruppi e gli utenti dell'organizzazione al gruppo locale Utenti Arcserve RHA come richiesto.

Quando si apre l'interfaccia utente, se un gruppo Utente con privilegi non è stato precedentemente selezionato, sarà necessario selezionarne un altro.

Nota: solo un utente con privilegi può modificare un server master. I server di replica possono essere modificati da un utente a cui è stato assegnato il ruolo Utente con privilegi, Admin o Controllo.

Come gestire gli utenti

Arcserve RHA consente di gestire le autorizzazioni utente per gli scenari mediante l'assegnazione di autorizzazioni delegate a utenti o gruppi.

I ruoli Utente con privilegi o Admin possono gestire i diritti degli utenti per ciascuno scenario. Dalla sezione relativa ai diritti degli utenti nell'interfaccia utente, è possibile impostare le autorizzazioni di amministrazione, controllo o visualizzazione di scenari per un utente o gruppo specifico. Tale gruppo o utente, dispone di conseguenza delle autorizzazioni relative a un determinato scenario e sarà in grado di gestire lo scenario sulla base dei diritti ad esso assegnati. Ad esempio, un utente o un gruppo può disporre di diritti utente per uno scenario e di diritti di amministratore per un altro scenario.

Delega dei diritti

I diritti utente vengono impostati per ogni singolo utente utilizzando la Gestione per apportare modifiche all'host master o alle repliche nella struttura di replica. I diritti utente vengono assegnati in base allo scenario.

È possibile assegnare autorizzazioni utente sui seguenti elementi:

Operazione	Super utente	Admin	Controllo	Solo visualizzazione
Impostazione dei diritti degli utenti	Sì	Sì	No	No

Operazione	Super utente	Admin	Controllo	Solo visualizzazione
Modifica di un host master	Sì	No	No	No
Modifica della modalità di replica	Sì	Sì	No	No
Modifica della modalità di pianificazione	Sì	Sì	Sì	No
Modifica della dimensione di uno spool master	Sì	No	No	No
Modifica di rapporti su un server master	Sì	Sì	No	No
Modifica di un host di replica	Sì	Sì	Sì	No
Modifica della dimensione di uno spool di replica	Sì	Sì	No	No
Esecuzione di uno scenario	Sì	Sì	Sì	No
Interruzione di uno scenario	Sì	Sì	Sì	No
Sincronizzazione di uno scenario	Sì	Sì	Sì	No
Ripristino dei dati	Sì	Sì	No	No
Modifica delle notifiche sul server master	Sì	Sì	No	No
Modifica delle notifica sul server di replica	Sì	Sì	No	No
Generazione di un rapporto delle differenze	Sì	Sì	Sì	Sì
Impostazione di un segnalibro	Sì	Sì	Sì	No
Visualizzazione di rapporti delle differenze	Sì	Sì	Sì	Sì
Esecuzione di risorse ad alta disponibilità	Sì	No	No	No
Verifica dello stato di uno scenario	Sì	Sì	Sì	Sì
Sospensione di una replica	Sì	Sì	Sì	No
Modifica dei rapporti sulla replica	Sì	Sì	No	No
Modifica del file trigger del server master	Sì	Sì	Sì	No
Modifica del file trigger del server di replica	Sì	Sì	Sì	No

Impostazione dei diritti degli utenti

È possibile impostare o ripristinare i diritti degli utenti per uno scenario specifico.

Nota: è necessario ripristinare i diritti degli utenti per tutti gli scenari a cui sono associate licenze diverse da una licenza di protezione delegata.

Per impostare i diritti degli utenti, procedere come segue:

1. Dal menu Scenario della Gestione Arcserve RHA, selezionare Scenario, quindi User rights (Diritti utente).

   Importante: Il menu Scenario include l'opzione aggiuntiva User rights. Questa opzione è disponibile solo per gli utenti che possiedono i diritti Utente con privilegi o Admin.

   Viene visualizzata la finestra Protezione contenente i diritti di ciascuno scenario.

2. Fare clic su Aggiungi.

   Viene visualizzata la finestra di dialogo Selezione utenti o gruppi.

3. Dall'elenco a discesa Cerca in, selezionare un dominio.

4. Selezionare l'utente o il gruppo richiesto.

   Nota: le selezioni di più utenti o gruppi non sono supportate.

5. Fare clic su Aggiungi, quindi su OK.

6. Dalla colonna Autorizzazione, impostare i diritti di accesso per un utente o un gruppo dall'elenco a discesa.

   Importante: Se un utente rimuove se stesso (ruolo Admin) dall'elenco della finestra Protezione, non disporrà più di alcun diritto sullo scenario corrente. Dopo aver riavviato la Gestione Arcserve RHA o dopo circa 10 secondi, lo scenario non sarà più visibile nell'elenco degli scenari.

Impostazione del gruppo utente con privilegi

È possibile modificare un gruppo utente con privilegi in qualsiasi momento.

Per modificare un gruppo utente con privilegi, procedere come segue:

1. Nella Gestione, visualizzare il menu **Scenario** e selezionare l'opzione **Imposta il gruppo utente con privilegi**.

   Viene visualizzata la finestra di dialogo **Imposta il gruppo utente con privilegi**.

2. Dall'elenco **Gruppi sul Servizio di controllo**, selezionare il gruppo al quale si desidera assegnare il gruppo Utenti con privilegi.

Capitolo 16: Gestione dei servizi

Arcserve RHA include anche un meccanismo che consente l'automazione della gestione e del controllo dei servizi critici per la disponibilità dell'applicazione. La gestione dei servizi viene configurata nella procedura guidata di creazione scenario ma può essere gestita anche manualmente dalla scheda Directory principali della Gestione Arcserve RHA.

La funzionalità di gestione servizi è progettata per fornire un framework per la protezione delle applicazioni che non possono essere protette da scenari Arcserve RHA dedicati (ad esempio, Microsoft SQL o SharePoint Server). Piuttosto che creare script personalizzati per la gestione dei servizi, Arcserve RHA è in grado di avviare, interrompere e attivare l'avanzamento in base allo stato del servizi specificati.

Nota: si tratta di una funzionalità non applicabile agli scenari file server.

Questa sezione contiene i seguenti argomenti:

Gestione servizi (a pagina 350)

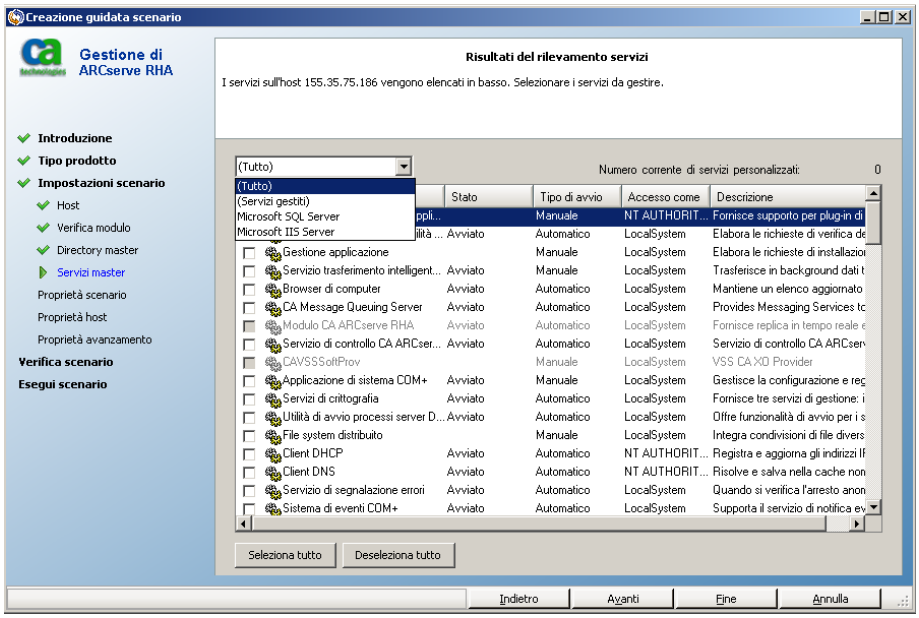
Gestione servizi

Nell'ambito della creazione o della modifica degli scenari, è possibile specificare i servizi da gestire. Durante la creazione di uno scenario, le schermate di gestione servizi vengono visualizzate durante la creazione guidata scenario. Per gli scenari esistenti, è possibile gestire i servizi anche dalla scheda Directory principali della Gestione Arcserve RHA.

I servizi rilevati sul server master specificato vengono visualizzati automaticamente sulla schermata dei risultati di rilevamento servizi nella creazione guidata scenario.

Le operazioni descritte di seguono fanno riferimento a scenari Applicazione personalizzata.

Per gestire i servizi:



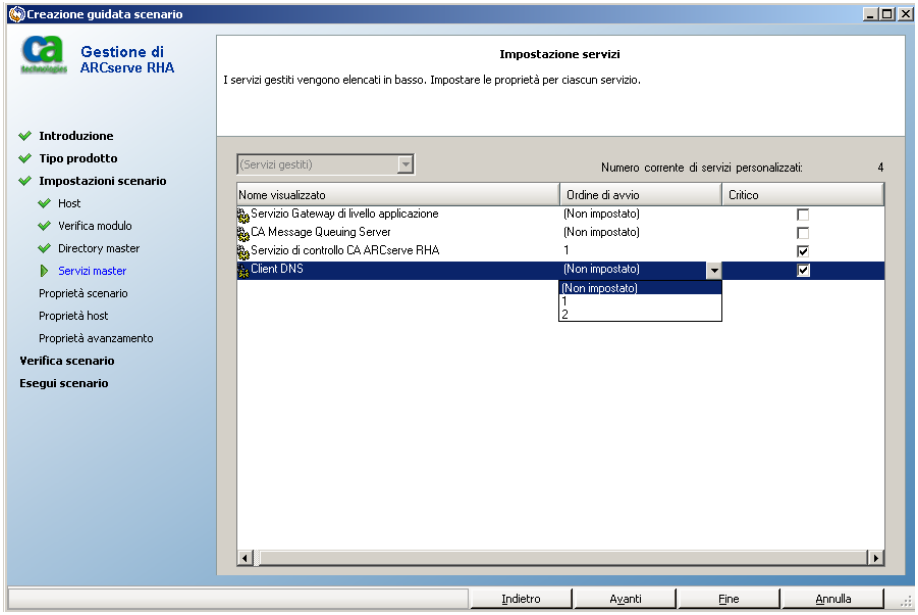
- **Tutto** - Elenca tutti i servizi rilevati sul server master
- **Servizi gestiti** - Elenca solo i servizi verificati
- **Database Oracle** - Elenca i servizi correlati ad Oracle se quest'ultimo è installato sull'host corrente
- **Microsoft SQL Server** - Elenca i servizi correlati a SQL se sull'host corrente è installato SQL Server
- **Microsoft IIS Server** - Elenca i servizi correlati a IIS se sull'host corrente è installato IIS Server
- **Microsoft SharePoint Server** - Elenca i servizi correlati a SharePoint se sull'host corrente è installato SharePoint Server

- **VMware vCenter Server** - Elenca i servizi correlati al server vCenter se sull'host corrente è installato vCenter Server
- **Microsoft Exchange Server** - Elenca i servizi correlati a Microsoft Exchange Server se quest'ultimo è installato sull'host corrente
- **Server di CRM di Microsoft Dynamics** - Elenca i servizi correlati a Microsoft Dynamics CRM Server se quest'ultimo è installato sull'host corrente

1. Selezionare un servizio da monitorare. Selezionare un servizio da monitorare facendo clic sulla casella a sinistra del servizio.

   Importante: Non utilizzare la Gestione servizi per controllare tutti i servizi sul server master in un unico scenario. Questo tipo di scenario non è concepito per proteggere la totalità del server.

2. Fare clic su Avanti per passare alla schermata delle impostazioni dei servizi.



3. Nella colonna Ordine di avvio specificare per ciascun servizio il valore numerico corrispondente all'ordine di avvio. Per i servizi per i quali l'ordine non è importante, utilizzare il valore predefinito (Non impostato). Le opzioni disponibili nel menu a discesa si aggiornano quando viene configurato il valore. Il primo servizio presenta solo due opzioni: Non impostato e 1. Il secondo servizio presenta tre opzioni: Non impostato, 1, 2 e così via. Se si assegna allo stesso ordine di avvio a due servizi, Arcserve RHA riordina automaticamente le selezioni effettuate.

4. Negli scenari di replica, la colonna Critico non è attiva. Negli scenari HA, utilizzare la colonna Critico per specificare se si desidera che il servizio attivi l'avanzamento in caso di errore. Per impostazione predefinita, tutti i servizi vengono contrassegnati come critici. Deselezionare la casella se non si desidera attivare il failover sul server in stand-by.

Capitolo 17: Gestione dei cluster

Arcserve RHA supporta cluster di dischi non condivisi. In tal modo vengono estese le funzionalità native di alta disponibilità agli ambienti cluster da LAN a WAN.

Questa sezione contiene i seguenti argomenti:

Introduzione ai miglioramenti apportati al cluster Windows 2008 (a pagina 353)
Funzionamento del supporto migliorato per i cluster Arcserve RHA (a pagina 354)
Distribuzione dei componenti Arcserve RHA per il supporto cluster (a pagina 354)
Replica di dati cluster e gestione di risorse (a pagina 363)
Ricerca di eventi (a pagina 366)

Introduzione ai miglioramenti apportati al cluster Windows 2008

Con Microsoft Cluster Services (MSCS) 2008, i cluster supportano i nodi in posizioni fisiche diverse, con o senza archiviazione condivisa, e gestiscono le operazioni di failover. Tuttavia, il disco condiviso per l'archiviazione dei dati cluster può essere un singolo punto di errore in caso di danneggiamento o perdita di dati.

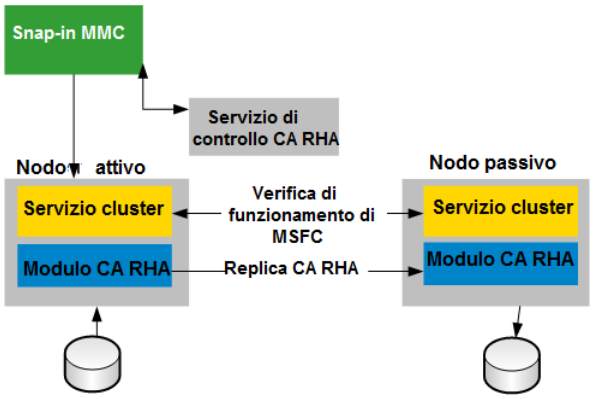
Arcserve RHA fornisce la replica di dati per i cluster di archiviazione condivisa.

Funzionamento del supporto migliorato per i cluster Arcserve RHA

Il nuovo plug-in di Arcserve RHA per il cluster di failover Microsoft (MSFC) 2008 consente di copiare i dati tra nodi cluster. Esistono tre ruoli relativi ai nodi:

- **Nodo di origine:** si tratta del nodo nel cluster per la comunicazione con la risorsa disco che si desidera proteggere.
- **Nodo di destinazione:** si tratta del nodo in cui si desidera copiare i dati.
- **Nodo inattivo:** si tratta del nodo in un cluster la cui comunicazione con una risorsa disco in un determinato periodo di tempo è disabilitata.

Per copiare i dati tra i nodi del cluster, è necessario creare una nuova risorsa, ovvero un disco RHA per l'archiviazione di dati replicati a partire dal nodo di origine. Se si desidera modificare le proprietà o monitorare lo stato di replica, è possibile gestire la nuova risorsa disco mediante la snap-in MMC. Il servizio di controllo Arcserve RHA (che deve essere installato su un server distinto) viene utilizzato per l'applicazione delle licenze. MSFC gestisce il failover nel cluster mentre Arcserve RHA esegue la replica delle risorse disco.



Distribuzione dei componenti Arcserve RHA per il supporto cluster

- Installazione di Arcserve RHA per i cluster di failover Microsoft (a pagina 355)
- Avvio di Arcserve RHA per i cluster di failover Microsoft (a pagina 355)
- Azioni della console (a pagina 356)

Installazione di Arcserve RHA per i cluster di failover Microsoft

Per installare Arcserve RHA per i cluster di failover, fare riferimento alla Guida all'installazione di Arcserve RHA.

Avvio di Arcserve RHA per i cluster di failover Microsoft

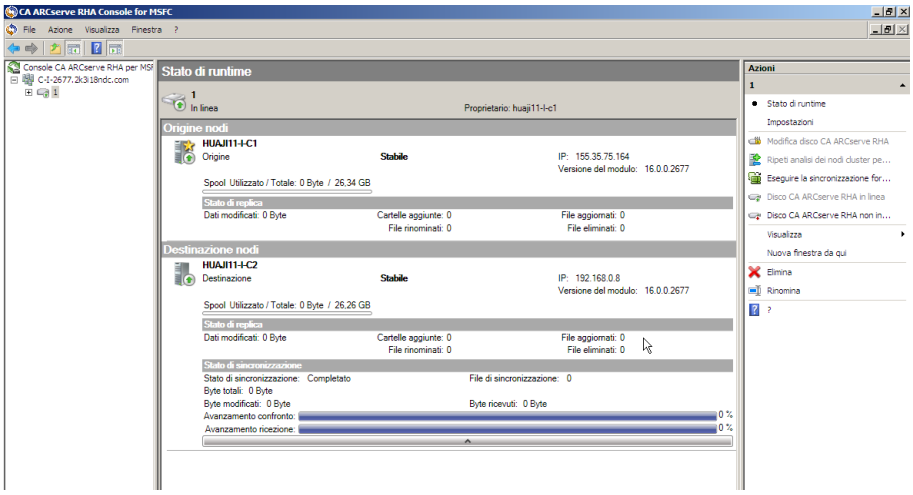
Dopo aver eseguito l'installazione, è possibile avviare il software dal menu Start di Windows.

È inoltre possibile integrare manualmente il software mediante la Gestione cluster di failover Microsoft.

Per integrare manualmente Arcserve RHA per i cluster di failover Microsoft

1. Fare clic su Start, Esegui e avviare mmc.exe.
2. Dal menu Console, fare clic su File, Aggiungi/Rimuovi snap-in.
3. Dall'elenco delle snap-in disponibili, selezionare la Console Arcserve RHA per MSFC, quindi aggiungerla all'elenco delle snap-in selezionate.
4. Selezionare Gestione cluster di failover, quindi aggiungerla all'elenco delle snap-in selezionate.
5. Fare clic su OK (Salva/Applica).

La struttura della directory principale verrà aggiornata per includere le snap-in specificate. A partire da questo momento è possibile gestire le risorse disco di Arcserve RHA.



Azioni della console

La console Arcserve RHA per il cluster di failover Microsoft consente di eseguire diverse azioni per la gestione e la verifica dello stato di replica. Le azioni disponibili dipendono dalla selezione effettuata nella Console. È inoltre possibile accedere a tali opzioni facendo clic con il tasto destro del mouse su un livello della struttura della console.

A livello della console

- **Apri cluster:** (a pagina 358) immettere un nome per il cluster, quindi fare clic su OK.
- **Visualizza: (a pagina 358)** fare clic su Personalizza per selezionare i componenti che si desidera visualizzare nella schermata Console, quindi fare clic su OK.
- **Nuova finestra:** (a pagina 358)consente di aprire una nuova finestra della console.
- **Aggiorna: (a pagina 359)** aggiorna la visualizzazione.
- **?: (a pagina 359)** consente di aprire la guida in linea della console.

A livello di cluster

- **Aggiungi disco Arcserve RHA:** (a pagina 359) consente di aprire la finestra di dialogo di aggiunta del disco. Fornire un nome disco e un volume facoltativo, quindi fare clic su OK.
- **Visualizza:** fare clic su Personalizza per selezionare i componenti che si desidera visualizzare nella schermata Console, quindi fare clic su OK.
- **Nuova finestra:** consente di aprire una nuova finestra della console.
- **Aggiorna:** aggiorna la visualizzazione.
- **?**: consente di aprire la guida in linea della console.

A livello della risorsa disco

- **Stato di runtime:** (a pagina 359) la console consente di verificare lo stato di runtime delle risorse disco del cluster. Vengono fornite informazioni relative allo Stato di replica, la Versione del modulo e lo Stato di sincronizzazione.
- **Impostazioni: (a pagina 360)** è possibile impostare le seguenti proprietà:
  - Tipo di sincronizzazione: sincronizzazione a livello di file o di blocchi. La sincronizzazione file è adatta alle applicazioni File server, mentre la sincronizzazione a blocchi è indicata per le applicazioni del database.
  - Ignora file della stessa dimensione/ora: Attivo o Non attivo. Si tratta di un filtro che consente il confronto dei dati: tiene in considerazione soltanto la dimensione dei file e l'ora di modifica in caso di differenza tra due file. Se impostato su Attivo, i file con lo stesso percorso, nome, dimensione e ora vengono ignorati. Si consiglia di disattivare questa proprietà se il tipo di sincronizzazione corrisponde a Sincronizzazione a blocchi.

- Replica attributo compresso NTFS: Attivo o Non attivo. Questa impostazione consente di replicare l'attributo compresso in file o directory durante la sincronizzazione e la replica.
- Replica elenchi di controllo: Attivo o Non attivo. Questa impostazione consente di replicare gli elenchi di controllo per file e directory durante la sincronizzazione o la replica.
- Replica NTFS ADS: Attivo o Non attivo.
- Numero di stream: valore predefinito impostato su 1. In ambienti WAN caratterizzati da un'ampia larghezza di banda e da un elevato livello di latenza, aumentare il numero di stream per migliorare l'utilizzo. Fare clic sulla freccia a discesa per impostare il valore o specificarlo nel file ws_rep.cfg.

- **Modifica disco Arcserve RHA:** (a pagina 360) consente di rinominare una risorsa disco esistente, impostare o modificare il volume facoltativo facendo clic su OK. È necessario rendere la risorsa disco non in linea per modificarla.
- **Ripeti analisi dei nodi cluster per la risorsa: (a pagina 361)** consente di aggiungere o rimuovere nodi host al cluster.
- **Eseguire la sincronizzazione forzata dei dati:** (a pagina 361) consente di eseguire la sincronizzazione immediata.
- **Disco Arcserve RHA in linea: (a pagina 362)** consente di portare in linea una risorsa disco. La sincronizzazione tra i nodi di origine e di destinazione viene eseguita automaticamente e le modifiche ai dati vengono replicate in tempo reale sul nodo di destinazione. L'avanzamento viene visualizzato nel riquadro Stato di runtime.
- **Disco Arcserve RHA non in linea: (a pagina 362)** consente di portare non in linea una risorsa disco in modo da poterla modificare. La replica dei dati viene interrotta quando la risorsa non è più in linea.
- **Visualizza:** Raggruppa per Ruolo o Raggruppa per Topologia. Il ruolo consente di visualizzare i dischi per stato. La topologia consente di visualizzare le assegnazioni dei dischi ai siti.
- **Nuova finestra:** consente di aprire una nuova schermata.
- **Elimina:** consente di rimuovere una risorsa disco.
- **Rinomina:** consente di modificare il nome della risorsa disco. La barra di evidenziazione diviene un rettangolo e il cursore viene attivato.
- **?:** consente di aprire la guida in linea al cluster.

Livello nodo

- **Visualizza:** fare clic su Personalizza per selezionare i componenti che si desidera visualizzare nella schermata Console, quindi fare clic su OK.
- **Nuova finestra:** consente di aprire una nuova finestra della console.
- **?**: consente di aprire la guida in linea della console.

Apertura di un cluster

Per aprire un cluster, è necessario selezionare Arcserve RHA per la voce MFC dall'elenco Directory principale.

1. Fare clic sulla console Arcserve RHA per il cluster di failover Microsoft dell'elenco Directory principale.
2. Dall'elenco Azioni, fare clic su Apri cluster.
3. Nella finestra di dialogo Apri cluster, immettere il nome del cluster e fare clic su OK.

   Il cluster viene visualizzato nella casella Licenza.

Personalizzazione della visualizzazione

L'opzione Visualizza consente di selezionare i componenti da visualizzare nella schermata della console. La stessa visualizzazione è disponibile a tutti i livelli della Directory principale.

Per personalizzare la visualizzazione

1. Dall'elenco Directory principale, selezionare Console, Cluster, Risorsa disco o Server ed evidenziare l'elemento.
2. Dall'elenco Azioni, fare clic su Visualizza.
3. Fare clic su Personalizza.
4. Fare clic per selezionare o deselezionare i componenti MMC e snap-in che si desidera visualizzare o nascondere, quindi fare clic su OK.

La visualizzazione viene modificata in base alle impostazioni.

Apertura di una nuova finestra

È possibile aprire altre finestre della console in base alle proprie necessità. Si tratta di un'azione disponibile per tutti i livelli della Directory principale, il cui comportamento corrisponde a quello del comando Microsoft.

Per aprire una nuova finestra

1. Dall'elenco Directory principale, fare clic sulla console, il cluster, la risorsa disco o il server.
2. Dall'elenco Azioni, fare clic su Nuova finestra.

   Viene visualizzata una nuova finestra. Utilizzare i controlli standard di Windows per ridurre, ingrandire o spostare la finestra in base alle proprie esigenze.

Aggiornamento della visualizzazione

È possibile aggiornare la visualizzazione a partire da tutte le selezioni della console.

Per aggiornare la visualizzazione

1. Fare clic su Aggiorna da qualsiasi livello della console.

Assistenza

È possibile ottenere informazioni relative a qualsiasi elemento selezionato nella console.

Per ottenere assistenza

1. Fare clic su? in qualsiasi selezione della console.

Aggiunta di una risorsa disco Arcserve RHA

È possibile creare una nuova risorsa disco di Arcserve RHA soltanto a partire dal livello di cluster dell'elenco Directory principale. Consultare la sezione Creazione di una nuova risorsa disco. (a pagina 365)

Visualizzazione dello stato di runtime

È possibile visualizzare lo stato delle risorse disco del cluster e ottenere informazioni quali lo stato della replica, la versione del modulo e lo stato della sincronizzazione.

L'azione Stato runtime è disponibile soltanto se la risorsa disco è selezionata nell'elenco Directory principale.

Per visualizzare lo stato di runtime

1. Fare clic sulla risorsa disco dell'elenco Directory principale.
2. Fare clic su Stato di runtime.

   Per impostazione predefinita, lo stato viene visualizzato per i ruoli di origine e di destinazione
3. (Facoltativo) Fare clic su Visualizza, Raggruppa per Topologia per visualizzare lo stato raggruppato per Siti.

Nota: le selezioni Raggruppa per Ruolo e Raggruppa per Topologia sono disponibili solo per l'azione Visualizza della risorsa disco.

Configurazione delle impostazioni del server

È possibile impostare le seguenti proprietà.

- **Tipo di sincronizzazione:** sincronizzazione a livello di file o di blocchi. La sincronizzazione file è adatta alle applicazioni File server, mentre la sincronizzazione a blocchi è indicata per le applicazioni del database.
- **Ignora file della stessa dimensione/ora:** Attivo o Non attivo. Si tratta di un filtro che consente il confronto dei dati: tiene in considerazione soltanto la dimensione dei file e l'ora di modifica in caso di differenza tra due file. Se impostato su Attivo, i file con lo stesso percorso, nome, dimensione e ora vengono ignorati. Si consiglia di disattivare questa proprietà se il tipo di sincronizzazione corrisponde a Sincronizzazione a blocchi.
- **Replica attributo compresso NTFS:** Attivo o Non attivo. Questa impostazione consente di replicare l'attributo compresso in file o directory durante la sincronizzazione e la replica.
- **Replica elenchi di controllo:** Attivo o Non attivo. Questa impostazione consente di replicare gli elenchi di controllo per file e directory durante la sincronizzazione o la replica.
- **Replica NTFS ADS:** Attivo o Non attivo.
- **Numero di stream:** valore predefinito impostato su 1. In ambienti WAN caratterizzati da un'ampia larghezza di banda e da un elevato livello di latenza, aumentare il numero di stream per migliorare l'utilizzo. Fare clic sulla freccia a discesa per impostare il valore o specificarlo nel file ws_rep.cfg.

Modifica delle risorse disco di Arcserve RHA

È possibile rinominare una risorsa disco esistente oppure impostare e modificare il volume.

Nota: per poter modificare una risorsa disco è necessario disattivarla.

Per modificare una risorsa disco Arcserve RHA

1. Dall'elenco Directory principale, selezionare la risorsa disco che si desidera modificare.
2. Fare clic su Disco Arcserve RHA non in linea.

   Attendere il completamento dell'operazione.
3. Se il colore dell'azione Modifica disco Arcserve RHA viene modificato (ovvero da grigio a nero), fare clic sull'azione.
4. Immettere un nuovo nome o un nuovo volume, quindi fare clic su OK.
5. Fare clic su Disco Arcserve RHA in linea

Ripetizione dell'analisi dei nodi cluster

Se sono stati aggiunti o rimossi nodi host da un cluster, sarà necessario riconfigurare la risorsa disco Arcserve RHA.

Per ripetere l'analisi dei nodi cluster

1. Selezionare la risorsa disco dall'elenco Directory principale.
2. Fare clic su Disco Arcserve RHA non in linea per interrompere la replica.
3. Fare clic su Ripeti analisi dei nodi cluster per la risorsa.
4. Fare clic su Disco Arcserve RHA in linea per riavviare la replica.

Esecuzione della sincronizzazione forzata

Quando una risorsa disco viene resa in linea, la sincronizzazione viene eseguita automaticamente. Tuttavia, è possibile eseguire la sincronizzazione in base alle proprie necessità, ad esempio prima di una sostituzione hardware.

Per imporre la sincronizzazione

1. Fare clic sulla risorsa disco dell'elenco Radice cluster.
2. Dall'elenco Azione, fare clic su Eseguire la sincronizzazione forzata dei dati.

Attivazione o disattivazione di una risorsa disco

Dopo aver creato una risorsa disco, è necessario applicare la licenza e metterla in linea per poter sincronizzare l'intero nodo di origine con la destinazione. Al completamento della sincronizzazione, tutte le modifiche ai dati verranno replicate in tempo reale sul nodo di destinazione. Lo stato di replica è disponibile nella visualizzazione dello stato di runtime.

Per modificare una risorsa disco, è necessario portarla non in linea. La replica è temporaneamente sospesa.

Per attivare o disattivare una risorsa disco

1. Selezionare la risorsa disco creata dall'elenco Directory principale.
2. Fare clic su Disco Arcserve RHA in linea.
3. Fare clic su Stato di runtime. Attendere che lo stato diventi In linea e Stabile. Lo stato di sincronizzazione viene avviato con l'inizializzazione. Una volta completata la sincronizzazione, lo stato passa a Completato.
4. Se si desidera disattivare la risorsa disco, fare clic su Disco Arcserve RHA non in linea.
5. Attendere durante l'interruzione della replica.
6. Fare clic su Stato di runtime, quindi verificare che lo stato sia Non in linea e Interrotto.

   La risorsa disco non è in linea.

   Quando si desidera riportare la risorsa disco allo stato precedente, selezionare la risorsa e fare clic su Disco Arcserve RHA in linea. È inoltre possibile eseguire la sincronizzazione forzata.

Replica di dati cluster e gestione di risorse

L'archiviazione cluster può corrispondere a un singolo punto di errore. Per proteggere i dati cluster, utilizzare Arcserve RHA per il cluster di failover Microsoft per replicare i dati su un altro disco. Il disco può essere remoto.

Visualizzazione cluster

- Apertura di un cluster (a pagina 363)
- Ricerca di cluster (a pagina 364)
- Personalizzazione della visualizzazione (a pagina 358)
- Apertura di una nuova finestra (a pagina 358)
- Aggiornamento della visualizzazione (a pagina 359)

Protezione archiviazione cluster

- Aggiunta di una risorsa disco Arcserve RHA (a pagina 359)
- Modifica delle risorse disco di Arcserve RHA (a pagina 360)
- Ripetizione dell'analisi dei nodi cluster (a pagina 361)
- Esecuzione della sincronizzazione forzata (a pagina 361)
- Configurazione delle impostazioni del server (a pagina 360)
- Visualizzazione dello stato di runtime (a pagina 359)
- Attivazione o disattivazione di una risorsa disco (a pagina 362)

Gestione delle licenze (a pagina 366)

Apertura di un cluster

Dopo aver configurato un cluster, è possibile gestirlo mediante la console Arcserve RHA per il cluster di failover Microsoft.

Per aprire un cluster

1. Fare clic con il tasto destro del mouse sulla console Arcserve RHA per il cluster di failover Microsoft.
2. Selezionare Apri cluster.
3. Specificare il nome del cluster, quindi fare clic su OK.

   Il cluster specificato viene caricato e viene visualizzato nel pannello.

Nota: è inoltre possibile aprire cluster dall'elenco Azioni situato nella parte destra della console.

Ricerca di cluster

Se si desidera visualizzare quali risorse disco sono contenute in un cluster specifico, o quali nodi cluster utilizzano una risorsa disco specifica, è possibile esplorare i cluster. È inoltre possibile determinare lo stato della risorsa disco e l'host del cluster.

Per cercare un cluster

1. Dalla Microsoft Management Console, espandere il nodo dell'ambito della radice del riquadro del nodo di ambito. Tutte le risorse disco vengono elencate nel nodo cluster.
2. Espandere il nodo disco di Arcserve RHA. Tutti i nodi host del cluster verranno visualizzati nella risorsa disco.

Creazione di una nuova risorsa disco

La snap-in MMC di Arcserve RHA consente di creare una nuova risorsa disco che funge da replica in uno scenario di Arcserve RHA. La risorsa disco di Arcserve RHA non supporta l'utilizzo di un disco quorum.

Per ogni modifica di un nodo cluster (espulsione o aggiunta di un nodo), si consiglia di rianalizzare i nodi cluster per la risorsa. Per ulteriori informazioni, consultare la sezione Ripetizione dell'analisi dei nodi cluster (a pagina 361).

Se più nodi cluster condividono dischi reali, verificare che venga utilizzata la stessa lettera di unità per tutti i nodi cluster durante la creazione della risorsa disco. Se il disco reale non è in linea, connetterlo alla console di gestione disco di Microsoft, quindi verificare che la lettera di unità prevista sia stata assegnata ai volumi appartenenti al disco. È possibile modificare la lettera di unità dalla console di gestione disco di Microsoft.

Nota: è possibile creare la risorsa disco senza dover completare il campo Volume di destinazione. Tuttavia, è necessario specificare l'informazione se si desidera portare la risorsa disco in linea. Se si desidera aggiungere le informazioni relative al volume in un secondo momento, fare clic sull'opzione Modifica disco Arcserve RHA.

Per creare una nuova risorsa disco

1. Dalla console Arcserve RHA per MSFC, fare clic sul nodo cluster.
2. Dall'elenco Azioni, fare clic su Aggiungi disco Arcserve RHA.
3. Specificare il nome del disco e il volume di destinazione, quindi fare clic su OK.

La risorsa disco viene creata al di sotto del nodo cluster nella console. I nodi che utilizzano la risorsa disco vengono rilevati automaticamente ed inseriti nell'elenco.

Passaggi successivi:

- Gestione delle licenze (a pagina 366)
- Aggiunta di risorse disco Arcserve RHA a servizi o applicazioni (a pagina 365)

Aggiunta di risorse disco ad applicazioni

Dopo aver creato una risorsa disco Arcserve RHA nella console di Arcserve RHA per la Gestione cluster di failover Microsoft (MSFC), creare una nuova applicazione tramite la configurazione di un servizio vuoto (Configure an Empty Service) o la creazione guidata di un'applicazione (Application Wizard) in MSFC, quindi aggiungere la risorsa creata.

Gestione delle licenze

Prima di applicare una licenza, è necessario creare una risorsa disco Arcserve RHA. Il numero di licenze deve corrispondere a quello dei nodi nel cluster e non a quello delle risorse disco di Arcserve RHA. Non è necessario applicare la licenza ogni volta che si crea una risorsa disco.

Per gestire le licenze

1. Dalla console di Arcserve RHA per il cluster di failover Microsoft, fare clic su Modifica server licenze per assegnare un server licenze. Se il server licenze è già stato assegnato, passare al passaggio 5.
2. Immettere l'indirizzo IP ed il numero di porta del server licenze, ovvero il server su cui è installato il Servizio di controllo di Arcserve RHA.
3. Fare clic su OK.
4. Immettere il nome utente e la password, quindi fare clic su OK.
5. Fare clic su Aggiorna licenze. Verrà visualizzata la finestra Aggiorna licenze. Immettere il nome utente e la password, quindi fare clic su OK.

Il numero di licenze viene aggiornato.

Nota: le prenotazioni delle licenze devono essere annullate manualmente prima dell'eliminazione di un cluster. In caso contrario, la chiave di licenza potrebbe andare persa. Fare clic su Aggiorna licenze per rilasciare le licenze esistenti.

Ricerca di eventi

Nell'interfaccia MMC, selezionare Eventi cluster per visualizzare i registri.

La finestra di dialogo di filtro degli eventi cluster consente di filtrare gli eventi in base ai seguenti elementi:

- Nodi
- Registri eventi
- Livello
- ID evento
- Intervallo date

Capitolo 18: Creazione ed esecuzione degli script definiti dall'utente

Sebbene la creazione degli scenari sia flessibile, facile da utilizzare ed intuitiva, a volte potrebbe essere necessario disporre di opzioni di personalizzazione più avanzate per aumentare le prestazioni del software. Gli script definiti dall'utente offrono tale grado di personalizzazione, consentendo di aggiungere operazioni agli scenari. Gli script vengono limitati solamente dal sistema operativo in uso. Se un file può essere eseguito dalla riga di comando su un host specifico, tale file può essere applicato come script in uno scenario.

Gli script sono compatibili con tutte le versioni di prodotto.

È possibile utilizzare i file batch (.bat o .cmd), VBScript (.vbs) con Cscript.exe, o gli script PowerShell (.ps) con Arcserve RHA. Arcserve RHAr12.x e versioni successive includono uno snap-in PowerShell. Gli script shell (. sh) possono essere utilizzati sui sistemi UNIX.

Esempio

È possibile creare un file batch (example.bat) che eseguono un file VBScript con Cscript. Per eseguire questa operazione, richiamare l'eseguibile Cscript e quindi trasmettere il file VBScript come file di chiamata. Specificare i nomi dei file batch nel campo Nome script (percorso completo) nella proprietà di scenario appropriata.

Questa sezione contiene i seguenti argomenti:

Funzionamento degli script definiti dall'utente con Arcserve RHA (a pagina 368)
Proprietà degli script definiti dall'utente (a pagina 368)

Funzionamento degli script definiti dall'utente con Arcserve RHA

La scrittura degli script utilizzati con Arcserve RHA e versioni precedenti deve restituire codici numerici che definiscano gli stati validi (0) e gli stati di errore (qualsiasi valore diverso da zero). Il software visualizza i codici restituiti nella finestra degli eventi per poter determinare immediatamente quando e dove si sono verificati gli errori.

Il formato degli script è il seguente:

```
NomeScript (percorso completo) Argomenti
```

Il nome dello script corrisponde al nome e al percorso completo dello script eseguibile che si desidera richiamare Aggiungere directory a questa proprietà con il seguente formato: <drive>:\<dir>\<file.ext>. Il software visualizza le directory come: <drive>:/<dir>/<file.ext>. Gli argomenti trasmessi allo script sono valori statici e letterali.

Gli script devono presentare lo stesso nome e risiedere nella stessa directory sia sul master che sul server di replica.

Nota: non è possibile eseguire script che attivano applicazioni di interfaccia utente su sistemi Windows a 64 bit.

È possibile eseguire gli script da diverse proprietà di scenario. Di seguito vengono descritte le procedure di impostazione e le proprietà degli script per ogni scenario.

Proprietà degli script definiti dall'utente

È possibile eseguire script definiti dall'utente nei seguenti riquadri delle proprietà:

- **Proprietà scenario** -- Notifica evento, Gestione rapporti
- **Proprietà master** -- Replica, Notifica evento, Gestione rapporti
- **Replica and Scheduled Task Properties (Proprietà replica e attività Pianificate)** -- Replica, Attività pianificate, Notifica evento, Gestione rapporti
- **Proprietà High Availability** -- Reindirizzamento traffico di rete, Funzionante, DB Application (Applicazione database), Azione per esito positivo
- **Assured Recovery Properties (Proprietà Assured Recovery)** -- Azione in caso di esito positivo della verifica (database in linea, database non in linea)

Esecuzione degli script definiti dall'utente da Proprietà scenario

Salvare gli script che si desidera eseguire da Proprietà scenario sull'host del Servizio di controllo.

Nota: gli script aggiunti a Proprietà scenario riguardano lo scenario, gli host master e di replica. Nel caso in cui uno script di gestione dei rapporti venga aggiunto in Proprietà scenario e ad un host dello scenario, lo script viene duplicato.

È possibile eseguire gli script dai seguenti gruppi di proprietà:

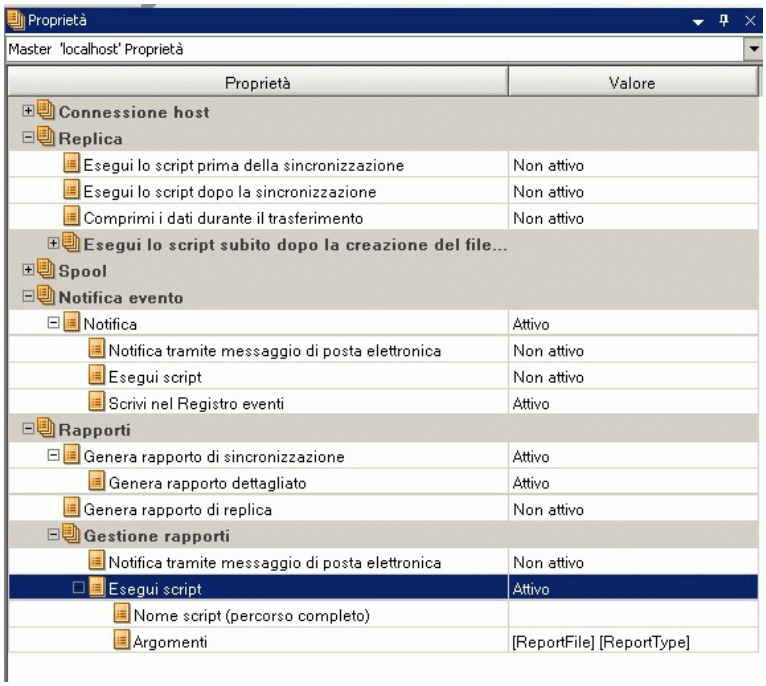
- **Notifica evento** -- Questo script consente la gestione di eventi o errori nel momento in cui si verificano. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.
- **Gestione rapporti** -- Questo script viene richiamato in seguito alla generazione di un rapporto. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.

Per specificare uno script di Proprietà scenario, si rimanda alla sezione Specificare uno script personalizzato in una Proprietà (a pagina 376).

Esecuzione di script definiti dall'utente da Proprietà master

Le proprietà master consentono di specificare gli script del server master.

È possibile eseguire gli script dai seguenti gruppi di proprietà:



Replica

- Se viene attivata la proprietà Esegui lo script prima della sincronizzazione, il processo di sincronizzazione non viene avviato fino al completamento dello script.
- Se viene attivata la proprietà Esegui lo script dopo la sincronizzazione, lo script viene eseguito sul master immediatamente dopo l'avvio della sincronizzazione. La sincronizzazione non attende il completamento dello script.
- Se viene attivata la proprietà Esegui lo script subito dopo la creazione del file trigger, (solo scenari file server), vengono eseguite le operazioni particolari definite nello script quando il file di trigger specificato viene visualizzato.

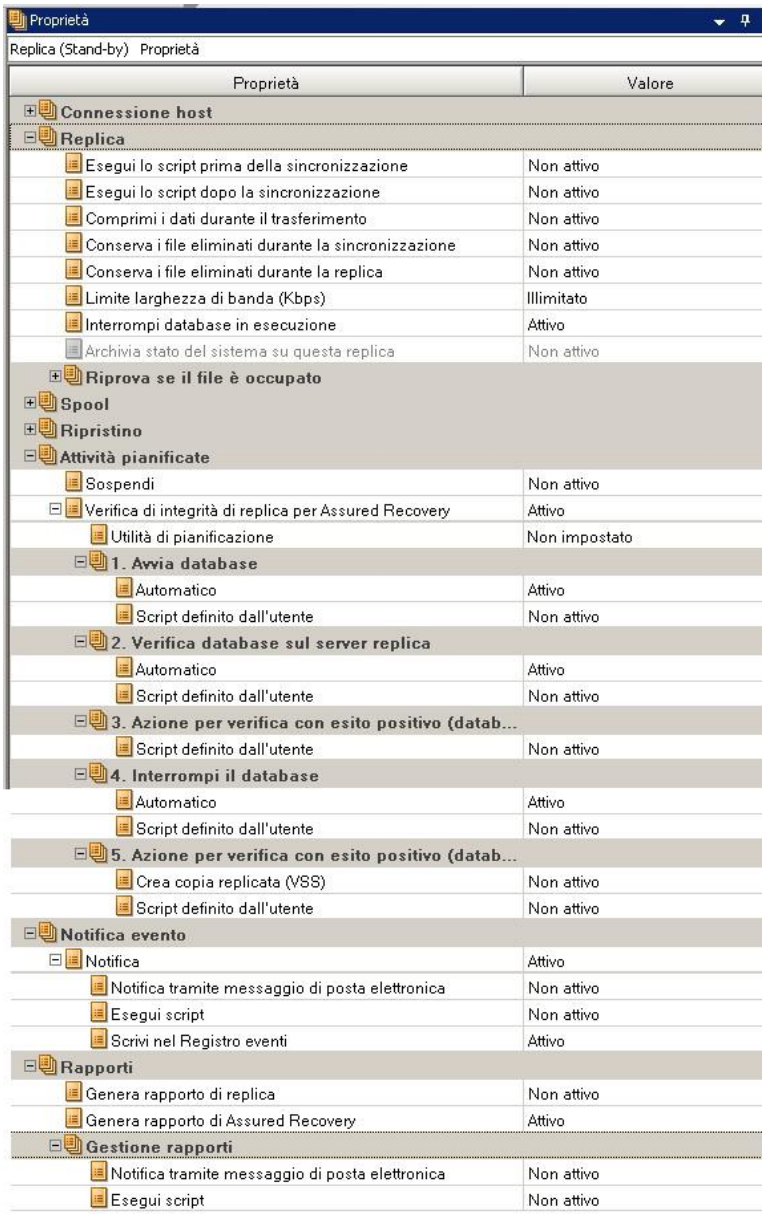
Notifica evento -- Questo script consente la gestione di eventi o errori nel momento in cui si verificano. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.

Gestione rapporti -- Questo script viene richiamato in seguito alla generazione di un rapporto. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.

Per specificare uno script in Proprietà master, si rimanda alla sezione Specificare uno script definito dall'utente in Proprietà. (a pagina 376)

Esecuzione di script definiti dall'utente da Proprietà di replica

È possibile eseguire gli script definiti dall'utente in esecuzione sul server di replica dai seguenti gruppi di proprietà:



Replica

- **Esegui lo script prima della sincronizzazione** -- attivare questa proprietà per l'esecuzione immediata di uno script sulla replica prima della sincronizzazione. La sincronizzazione non viene avviata fino al completamento dello script che può essere utilizzato per l'avvio di determinati servizi di terze parti.

- **Esegui lo script dopo la sincronizzazione** -- Attivare questa proprietà per l'esecuzione immediata di uno script sulla replica dopo la sincronizzazione. Non viene atteso il completamento della sincronizzazione.

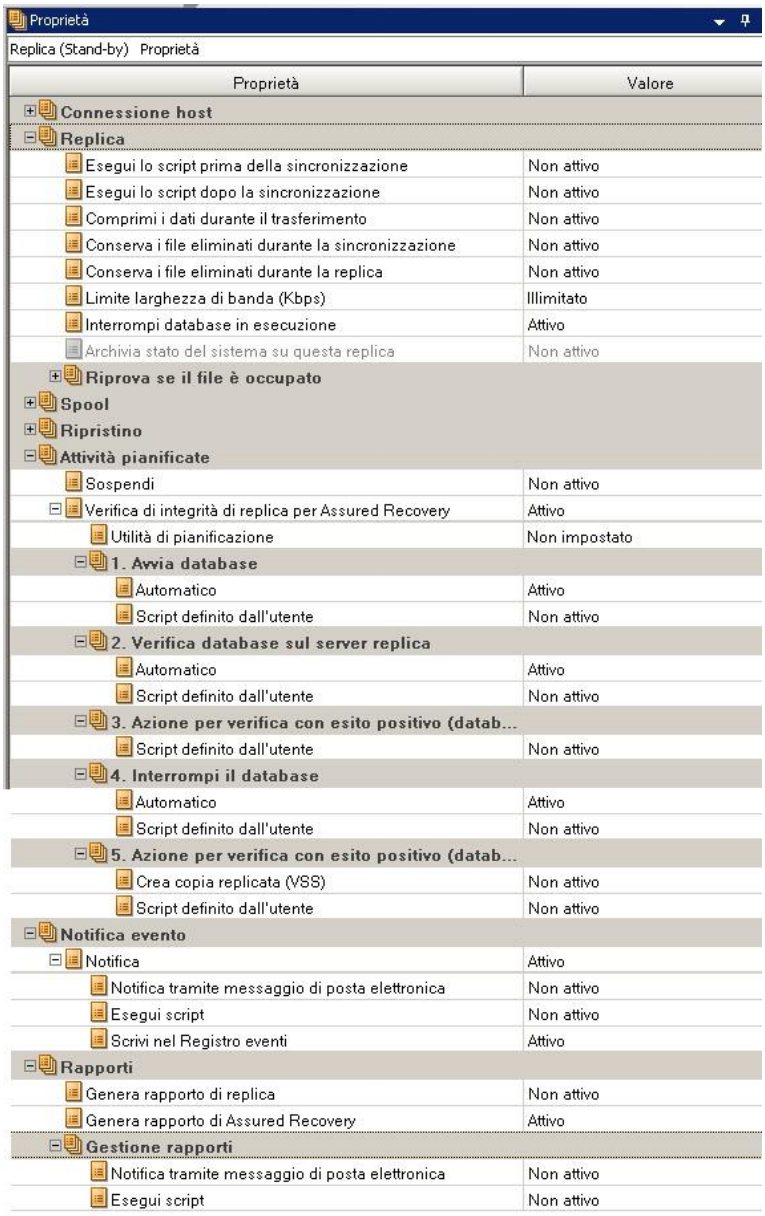
- **Notifica evento --** questo script consente di personalizzare la gestione di eventi e errori. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.

Gestione rapporti -- Questo script viene eseguito dopo la generazione di un rapporto. Attivare la proprietà Esegui script. Immettere il nome nel campo Nome script (percorso completo). Fornire gli argomenti da trasmettere allo script nel campo Argomenti.

Per specificare uno script in Replica and Scheduled Task Properties (Proprietà replica e attività pianificate), si rimanda alla sezione Specificare uno script definito dall'utente in Proprietà. (a pagina 376)

Esecuzione degli script definiti dall'utente da Proprietà delle attività pianificate.

È possibile eseguire gli script definiti dall'utente che vengono eseguiti in caso di esito positivo della verifica:



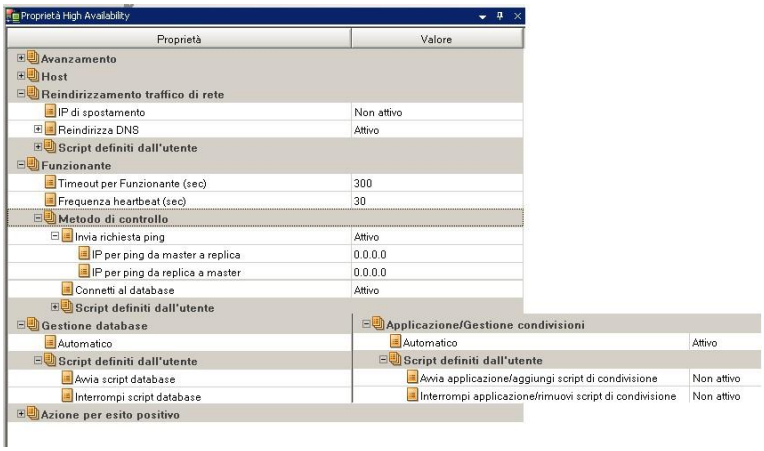
Attività Pianificate -- Verifica di integrità di replica per Assured Recovery

- **Avvia database** -- Se la proprietà Automatico è attivata, la proprietà Avvia database determina il primo passaggio del processo Assured Recovery, avviando i servizi di database sulla replica. Lo script viene eseguito quando i servizi vengono avviati e il database viene montato. Il processo Assured Recovery viene sospeso fino al completamento dello script. Se la proprietà Automatico è impostata su Non attivo e lo script definito dall'utente è impostato su Attivo è possibile specificare uno script per la sostituzione del primo passaggio standard.
- **Verifica database sul server di replica** -- Se viene attivata la proprietà Automatico, la proprietà Verifica database sul server di replica definisce il secondo passaggio nel processo Assured Recovery, verificando il corretto avvio di tutti i servizi di applicazione e che tutti i database siano stati montati correttamente e la validità del loro stato. Ad esempio, tale proprietà può essere utilizzata per l'esecuzione di una verifica DBCC del set di dati su SQL server. La verifica di integrità viene sospesa fino al completamento corretto dello script. In caso contrario, anche la verifica Assured Recovery avrà esito negativo. Se la proprietà Automatico è impostata su Non attivo e lo script definito dall'utente è impostato su Attivo è possibile sostituire il secondo passaggio standard.
- **Actions upon Successful Test (DB Online) (Azioni in caso di esito positivo della verifica (database in linea)**-- Dopo la corretta verifica della replica, i dati si trovano in uno stato valido. Questa proprietà consente di utilizzare questo tipo di informazione. Ad esempio, è possibile garantire l'esecuzione del backup su dati convalidati. Oppure assicurare l'esecuzione di un'applicazione.
- **Interrompi il database** -- Questa proprietà determina la fase finale della verifica Assured Recovery standard e interrompe i servizi di database al termine della verifica. Per sostituire la verifica standard, disattivare la proprietà Automatico e attivare lo script definito dall'utente. Utilizzare questa proprietà per interrompere qualsiasi processo avviato da uno script nella proprietà Avvia database.
- **Action Upon Success (DB Offline) (Azione in caso di esito positivo della verifica (database non in linea) --** Dopo la verifica corretta della replica, i dati si trovano in uno stato valido ed è possibile effettuarne una copia, il backup o acquisire una snapshot. Se si desidera eseguire un'operazione che non richiede l'esecuzione del database, utilizzare questa proprietà per registrare lo script. Se il sistema in esecuzione è Windows Server 2003 (o versioni successive) è possibile acquisire automaticamente le snapshot VSS.

Per specificare uno script, si rimanda alla sezione Specificare uno script definito dall'utente in Proprietà. (a pagina 376)

Esecuzione dello script definito dall'utente da Proprietà High Availability

È possibile eseguire lo script per scenari HA dai seguenti gruppi di proprietà:



- **Reindirizzamento del traffico di rete**
  - **Reindirizzamento da Attivo a Stand-by** -- attivare questa proprietà per eseguire uno script sul server attivo, se disponibile, per il reindirizzamento degli utenti all'host in stand-by oppure per rilasciare le risorse di rete sull'host attivo.
  - **Reindirizzamento da Stand-by ad Attivo** -- attivare questa proprietà per eseguire uno script sul server in stand-by, per il reindirizzamento degli utenti al server attivo.
  - **Identify Network Traffic Redirection (Individua reindirizzamento traffico di rete)** -- Attivare questa proprietà per l'esecuzione di uno script che determini quale server è attivo. Se lo script restituisce 0, l'host di esecuzione dello script viene considerato come il server attivo. Se lo script restituisce un valore diverso da zero, l'host viene considerato inattivo.
- **Metodo di controllo Funzionante**
  - **Verifica script sull'host attivo** -- Questo script viene eseguito sul server attivo durante gli heartbeat funzionanti per verificare che il server è disponibile agli utenti.
  - **Verifica script sull'host in stand-by** -- Questo script viene eseguito sul server in stand-by durante gli heartbeat funzionanti per verificare che il server è disponibile agli utenti.
  - **Avvia il database/Start Application/Add Shares (Avvia applicazione/Aggiungi condivisione)** -- Se attivata, lo script aumenta o sostituisce l'avvio dei servizi e delle applicazioni di database, o abilita la condivisione cartelle. L'azione definita viene realizzata durante il processo di esecuzione dello scenario sull'host attivo oppure durante un avanzamento sull'host in stand-by.

- **Avvia il database/Stop Application/Remove Shares (Interrompi applicazione/Aggiungi condivisione)** -- Se attivata, lo script aumenta o sostituisce l'arresto dei servizi e delle applicazioni di database, o disabilita la condivisione cartelle. L'azione definita viene realizzata durante il processo di esecuzione dello scenario sull'host in stand-by oppure durante un avanzamento sull'host attivo.

- **Azione per esito positivo** -- Se impostata su Attivo, lo script esegue le azioni definite dopo il completamento della procedura di avanzamento.

Specificare uno script definito dall'utente in Proprietà

La seguente procedura descrive la modalità di abilitazione degli script definiti dall'utente dalle diverse proprietà. È possibile abilitare più di uno script. Si consiglia di prestare attenzione se si sceglie di specificare script per scopi diversi. È possibile specificare gli script Gestione rapporti e Notifica evento in più gruppi di proprietà determinando una doppia esecuzione.

Per specificare uno script personalizzato in una proprietà:

1. Interrompere lo scenario se è in esecuzione.
2. Selezionare la scheda Proprietà appropriata per il server desiderato. Per ulteriori informazioni, consultare la sezione Proprietà degli script definiti dall'utente (a pagina 368).
3. Espandere il gruppo di proprietà desiderato.
4. Impostare la proprietà appropriata in base alle istruzioni fornite nelle sezioni corrispondenti all'esecuzione degli script definiti dall'utente.
5. Ripristinare l'esecuzione dello scenario.

Uso dello script di risoluzione dei problemi

Viene visualizzato un codice di errore (1) quando lo script VBS con cscript.exe viene eseguito.

Il codice di errore (1) relativo a uno script indica che un parametro non è valido oppure che non è possibile trovare lo script. Controllare gli argomenti dello scenario e verificare che la sintassi sia corretta e che tutti i caratteri, in particolare i simboli virgoletta, siano presenti. A volte, durante le operazioni di copia e incolla nel campo Argomenti dello scenario, le virgolette vengono considerate caratteri letterali speciali e non vengono visualizzate correttamente nel file cscript.exe durante l'esecuzione.

Viene visualizzato un messaggio di errore, ER00160: Lo script <nome script> non ha completato l'esecuzione in <numero> "secondi" durante l'avanzamento.

Questo problema può verificarsi quando uno script High Availability supera il periodo di timeout previsto per il completamento. Il valore di tempo predefinito è 300 secondi (5 minuti). È possibile modificare il file ws_rep.cfg nella directory di installazione del modulo per regolare il valore di timeout. L'attributo da modificare è HAScriptExecutionTimeout=300. Per modificare questo valore, eliminare il simbolo # presente davanti all'attributo, cambiare il valore numerico di destra, e quindi riavviare il servizio del modulo.

Viene visualizzato l'errore, ER00564: Script<script> inesistente oppure il messaggio di errore ER00569: Script<script> non trovato.

Ciò significa che lo script da eseguire non si trova nella posizione specificata. Controllare che non vi siano spazi all'interno della directory principale. Nel caso in cui fossero presenti degli spazi, sarà necessario includere la directory dello script tra virgolette, ad esempio: "c:\Program Files\ScriptExamples".

Viene visualizzato l'errore:Verifica script su host in stand-by non riuscita, oppure Verifica script su host attivo non riuscita.

Ciò significa che lo script Funzionante ha restituito un codice di errore sull'host specificato e che verrà eseguito un avanzamento oppure che sarà necessario eseguire un avanzamento.

Durante l'avvio dello scenario viene visualizzato l'errore: ERRORE: Il traffico di rete viene diretto sull'host <host>, ma l'applicazione è in esecuzione sull'host <host>.

È possibile che gli script Identify Network Traffic Redirection (Individua reindirizzamento traffico di rete) restituiscano valori incorretti. Assicurarsi che lo script sull'host attivo restituisca 0 e l'host in stand-by restituisca valori diversi da zero.

Durante l'avvio dello scenario viene visualizzato l'errore: ERRORE: Impossibile eseguire lo scenario.

È possibile che gli script Identify Network Traffic Redirection (Individua reindirizzamento traffico di rete) restituiscano valori identici. Assicurarsi che lo script sull'host attivo restituisca 0 e l'host in stand-by restituisca valori diversi da zero.

Durante l'avvio dello scenario,viene visualizzato l'avviso: AVVISO: Impossibile connettersi a <host> del server <master o di replica>, e l'errore: ERRORE: Nessuna informazione per <master o replica> da verificare ulteriormente.

Il modulo non può individuare lo script Identify Network Traffic Redirection (Individua reindirizzamento traffico di rete) sul master o sulla replica.

Capitolo 19: Configurazione dell'utilità NAT per RHA per impostazioni di rete diverse

Utilizzare l'utilità NAT per RHA se si dispone di un'impostazione di rete con firewall, server proxy o entrambi. Questo tipo di impostazioni di rete limitano l'accesso a determinati host e non consentono la creazione di scenari. Gli esempi riportati di seguito descrivono la procedura di configurazione dell'utilità NAT per impostazioni di rete diverse.

Questa sezione contiene i seguenti argomenti:

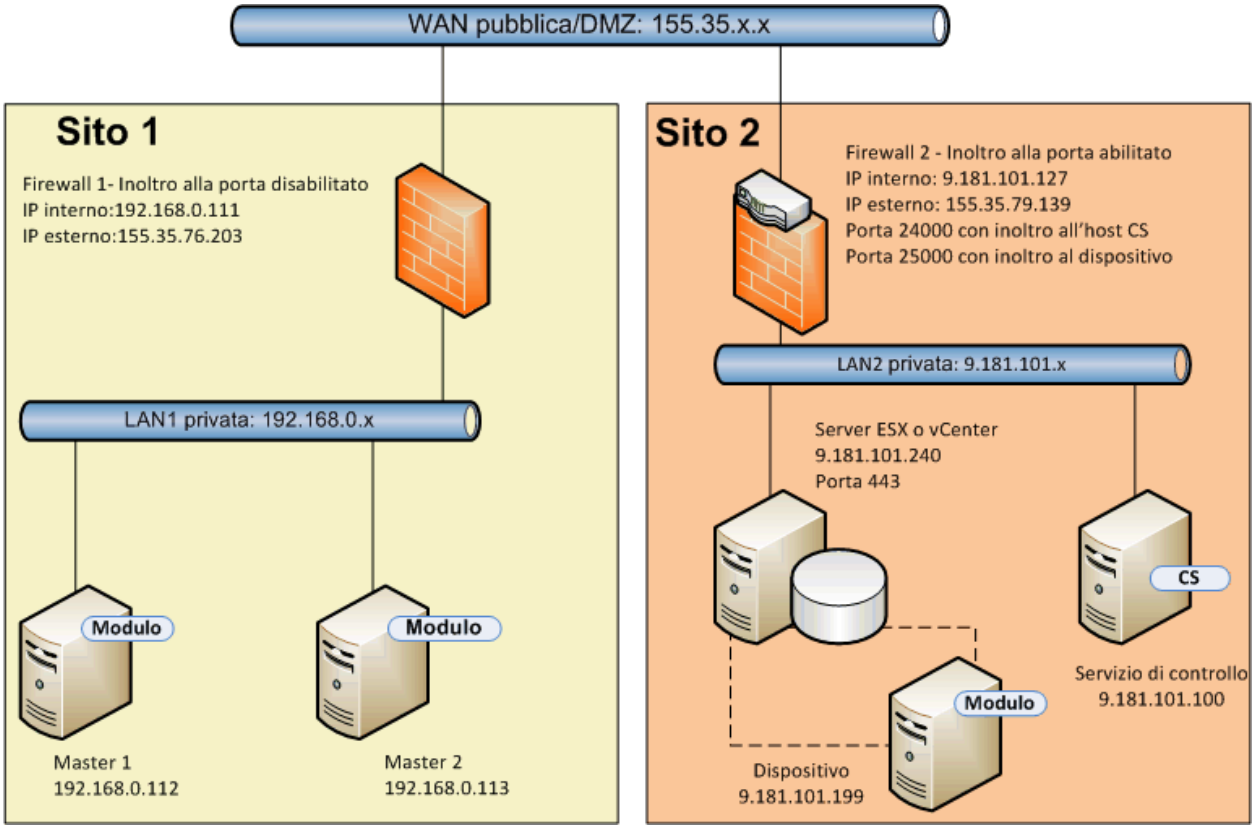
Esempio 1: Master protetti da firewall chiuso (a pagina 380)
Esempio 2: Master protetti da firewall chiuso con un server proxy (a pagina 387)
Esempio 3: Dispositivo e CS protetti da firewall chiuso (a pagina 390)
Esempio 4: Servizio di controllo su WAN pubblica (a pagina 393)
Esempio 5: Master, dispositivo e Servizio di controllo protetti da firewall con inoltro alla porta (a pagina 394)

Esempio 1: Master protetti da firewall chiuso

In questo esempio, il Servizio di controllo (CS) e il dispositivo non possono accedere al master. Di seguito viene descritta l'impostazione di rete.

- I master sono inclusi in una rete LAN privata protetta da firewall (Firewall 1) con inoltro alla porta disabilitato.
- Gli host in LAN 1 possono accedere alla WAN pubblica mediante il Firewall 1.
- Il Servizio di controllo e la replica sono inclusi in una rete LAN protetta da firewall (Firewall2) con inoltro alla porta abilitato.
- Gli host in LAN 2 possono accedere alla WAN pubblica mediante il Firewall 2. L'inoltro alla porta per il Firewall 2 configurato nel seguente modo:
  - La porta 24000 esegue l'inoltro all'host del Servizio di controllo.
  - La porta 25000 esegue l'inoltro al dispositivo.
- Entrambe le reti LAN private vengono connesse mediante una WAN pubblica.

Il seguente diagramma mostra l'impostazione di rete:



Nel caso in cui venga creato uno scenario HA per sistemi completi senza l'utilità NAT, si verificano le condizioni seguenti:

1. Il Servizio di controllo non è in grado di accedere al master in LAN1 in quanto il Firewall 1 non dispone dell'inoltro alla porta. Non è possibile creare uno scenario se il Servizio di controllo non è in grado di accedere al master.
2. Durante l'esecuzione di uno scenario precedente, i dati vengono copiati dal dispositivo o dal computer virtuale di avanzamento sul Sito 2 al master sul Sito 1. La replica dei dati non è possibile in quanto il Servizio di controllo non può eseguire l'accesso a Master 1.

Per creare uno scenario per questa impostazione di rete, utilizzare l'utilità NAT per RHA sul Master 1.

Di seguito si riportano le attività da eseguire per la configurazione dell'utilità NAT sul master durante la creazione di scenari e l'esecuzione del ripristino bare metal.

- Creazione di uno scenario HA per sistemi completi (a pagina 382)
- Esecuzione del ripristino bare metal da un punto di ripristino (a pagina 384)
- Esecuzione del ripristino bare metal mediante la replica inversa (a pagina 385)

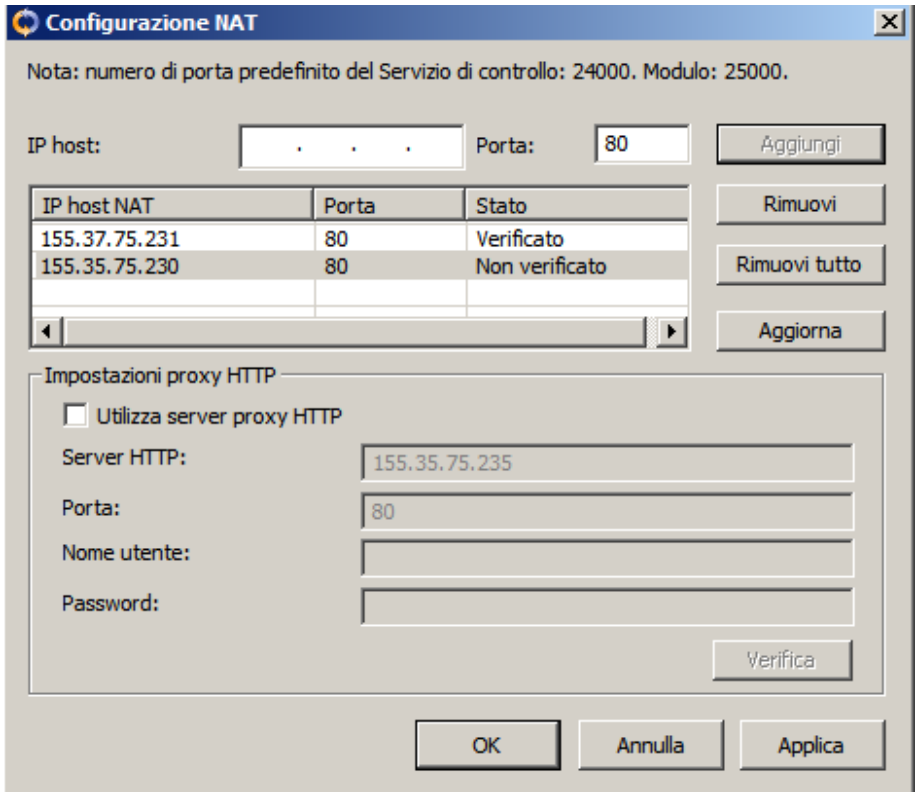
Creazione di uno scenario HA per sistemi completi

Prima di creare lo scenario HA per sistemi completi, eseguire le operazioni seguenti sul Master 1.

1. Eseguire l'utilità NAT per RHA dalla cartella del modulo.
2. Immettere l'indirizzo IP esterno, 155.35.79.139, e i numeri di porta del Firewall 2.

   Nota: il Servizio di controllo e il dispositivo sul Sito 2 vengono inoltrati dallo stesso indirizzo IP esterno (155.35.79.139) ma con porte differenti. È quindi necessario aggiungere le seguenti voci per ciascuna porta:

   - 155.35.79.139, 24000
   - 155.35.79.139, 25000



3. Fare clic su OK per applicare la configurazione.
4. Aprire la Gestione di RHA e fare clic su Nuovo sulla barra degli strumenti standard per creare lo scenario.
5. Selezionare Sistema completo e il tipo di prodotto, HA o AR.
6. Immettere l'indirizzo IP (192.168.0.112) e il numero di porta predefinito (25000) del master.
7. Immettere l'indirizzo IP (9.181.101.240) della piattaforma virtuale e il numero di porta predefinito (443).
8. Immettere l'indirizzo IP (155.35.79.139) del dispositivo e il numero di porta (25000). Questa porta dispone dell'inoltro alla porta per il dispositivo (9.181.101.199).

   Nota: se si seleziona Verifica Modulo Arcserve RHA sugli host, viene visualizzato un messaggio che informa l'utente che il modulo RHA non è installato su 155.35.79.139. La visualizzazione di questo messaggio di errore è dovuta all'elaborazione della verifica sul Firewall 2.
9. Immettere dettagli del volume, del pool di risorse, dell'archiviazione, delle proprietà di scenario e delle proprietà host simili a quelli di uno scenario di sistema completo.
10. Selezionare il tipo di avanzamento ed eseguire lo scenario.

Esecuzione del ripristino bare metal da un punto di ripristino

Il ripristino bare metal consente di recuperare dati e applicazioni da un punto di ripristino del segnalibro su un computer bare metal. Avviare il computer bare metal e configurare l'utilità NAT.

Procedere come descritto di seguito:

1. Interrompere lo scenario dalla Gestione RHA.
2. Avviare il Master 2 (computer bare metal) utilizzando il DVD di ripristino bare metal di RHA o l'immagine ISO.
3. Verificare le impostazioni della scheda di rete. Se le impostazioni non sono corrette, eseguire la configurazione manuale.
4. Aprire il prompt dei comandi e accedere alla cartella di RHA. Eseguire il comando seguente per aprire l'utilità NAT per RHA.

   ```
   natutil
   ```

5. Eseguire il comando seguente per aggiungere l'indirizzo IP esterno del Firewall 2 e i dettagli della porta.

   ```
   nat.addhost 155.35.79.139 24000
   ```

   ```
   nat.addhost 155.35.79.139 25000
   ```

   Porta 24000 per il Servizio di controllo e porta 25000 per il dispositivo.
6. Eseguire il comando seguente per applicare le impostazioni e stabilire una connessione tra il Master 2 e il Servizio di controllo.

   ```
   nat.apply
   ```

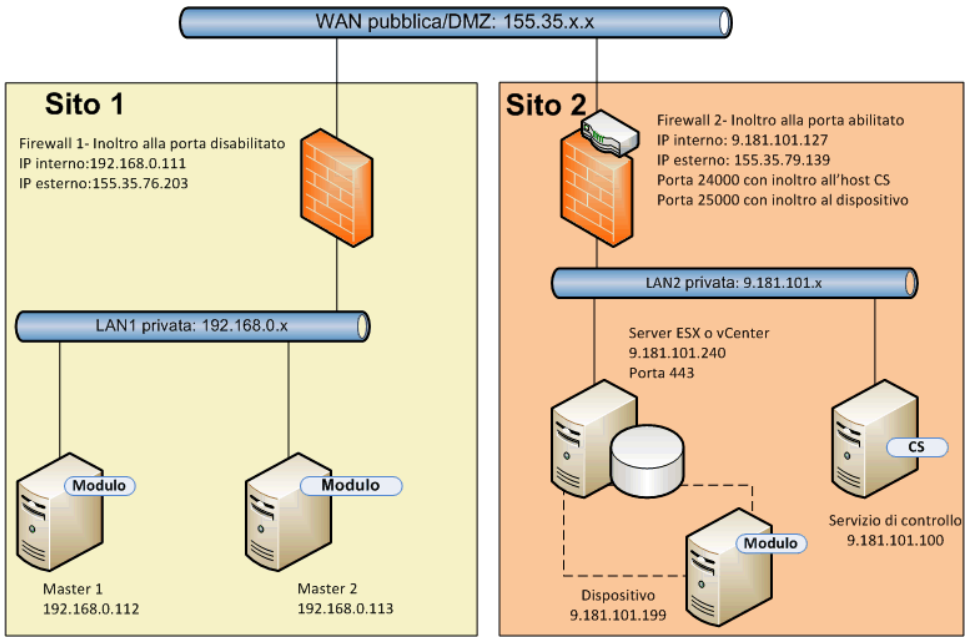
7. Aprire la Gestione di RHA e fare clic su Nuovo sulla barra degli strumenti standard per creare lo scenario.
8. Fare clic su Ripristina dati per aprire la procedura guidata di ripristino dei dati.
9. Selezionare il tipo di recupero (Ripristino bare metal) e il punto di ripristino.
10. Immettere l'indirizzo IP seguente e i dettagli della porta nella pagina Destinazione di recupero.

    IP di destinazione: 192.168.0.113, 25000
11. Fare clic su Verifica per verificare l'host di destinazione.
12. Immettere dettagli del volume, del pool di risorse, dell'archiviazione, delle proprietà di scenario e delle proprietà host simili a quelli di uno scenario di sistema completo.
13. Fare clic su Esegui per avviare lo scenario di recupero.

Esecuzione del ripristino bare metal mediante la replica inversa

Per questa impostazione di rete, è possibile eseguire il recupero dell'applicazione e dei dati in seguito a un failover utilizzando la replica inversa. In seguito a un failover o a un avanzamento, viene visualizzato un pulsante rosso Esegui che consente di avviare il processo di replica inversa. Viene creato un nuovo computer virtuale di avanzamento Questo computer virtuale contiene gli stessi dati del master ma presenta un indirizzo IP diverso (9.181.101.152 invece di 192.168.0.112).

Nell'esempio seguente, l'avanzamento si trova tra il computer virtuale di avanzamento sul Sito 2 e il computer bare metal (Master 2) sul Sito 1. Per consentire l'accesso a questo computer virtuale di avanzamento, impostare un nuovo inoltro di porta (25001) sul Firewall 2.



Ora si dispone del Servizio di controllo, del dispositivo e di un nuovo computer virtuale di avanzamento. Immettere i dettagli di questi tre computer nell'utilità NAT del master.

Procedere come descritto di seguito:

1. Avviare il computer bare metal (Master 2) mediante il DVD del ripristino bare metal o l'immagine ISO.
2. Verificare le impostazioni della scheda di rete. Se le impostazioni non sono corrette, eseguire la configurazione manuale.
3. Aprire il prompt dei comandi e accedere alla cartella di RHA. Eseguire il comando seguente per aprire l'utilità NAT per RHA.

   ```
   natutil
   ```

4. Eseguire il comando seguente per aggiungere l'indirizzo IP esterno del Firewall 2 e i dettagli della porta.

   ```
   nat.addhost 155.35.79.139 24000
   ```

   ```
   nat.addhost 155.35.79.139 25000
   ```

   ```
   nat.addhost 155.35.79.139 25001
   ```

   Porta 24000 per il Servizio di controllo, porta 25000 per il dispositivo e porta 25001 per il computer virtuale di avanzamento.
5. Eseguire il comando seguente per applicare le impostazioni e stabilire una connessione tra il master, il Servizio di controllo e il dispositivo.

   ```
   nat.apply
   ```

6. Aprire la Gestione RHA per creare lo scenario precedente. Selezionare lo scenario che ha eseguito l'avanzamento e fare clic su Esegui per aprire la procedura guidata di ripristino dei dati.
7. Immettere l'indirizzo IP seguente e i dettagli della porta nella pagina Replica inversa.

   IP/Nome origine: 155.35.79.139, 25001

   IP di destinazione: 192.168.0.113, 25000
8. Fare clic su Verifica per verificare l'host di destinazione.
9. Immettere dettagli del volume, del pool di risorse, dell'archiviazione, delle proprietà di scenario e delle proprietà host simili a quelli di uno scenario di sistema completo.
10. Fare clic su Esegui per avviare lo scenario precedente ed eseguire il processo di replica inverso.

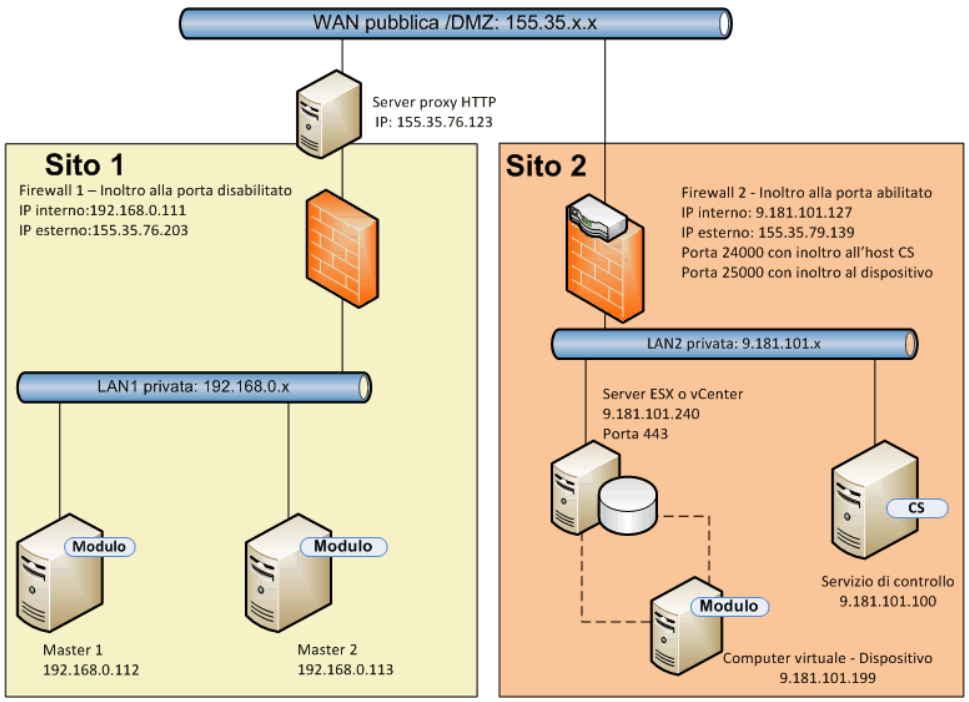
Una volta completata la sincronizzazione, avviare la regressione manuale per attivare il computer bare metal (Master 2).

Esempio 2: Master protetti da firewall chiuso con un server proxy

Questo esempio è simile all'Esempio 1, l'unica differenza è costituita dalla presenza di un server proxy aggiuntivo sul Sito 1. Di seguito viene descritta l'impostazione di rete.

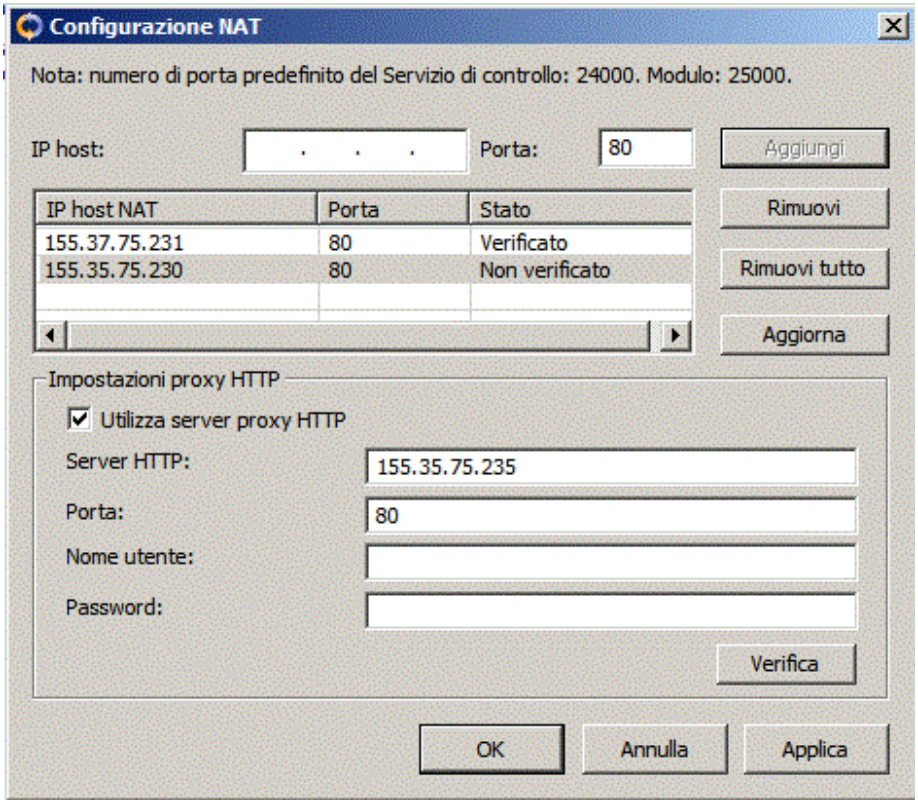
- I master sono inclusi in una rete LAN privata protetta da firewall (Firewall 1) con inoltro alla porta disabilitato.
- Il firewall 1 è connesso a un server proxy (155.35.76.123).
- Gli host in LAN 1 possono accedere alla WAN pubblica mediante il Firewall 1.
- Il Servizio di controllo e la replica sono inclusi in una rete LAN protetta da firewall (Firewall2) con inoltro alla porta abilitato.
- Gli host in LAN 2 possono accedere alla WAN pubblica mediante il Firewall 2. L'inoltro alla porta per il Firewall 2 configurato nel seguente modo:
  - La porta 24000 esegue l'inoltro all'host del Servizio di controllo.
  - La porta 25000 esegue l'inoltro al dispositivo.
- Entrambe le reti LAN private vengono connesse mediante una WAN pubblica.

Il seguente diagramma mostra l'impostazione di rete:

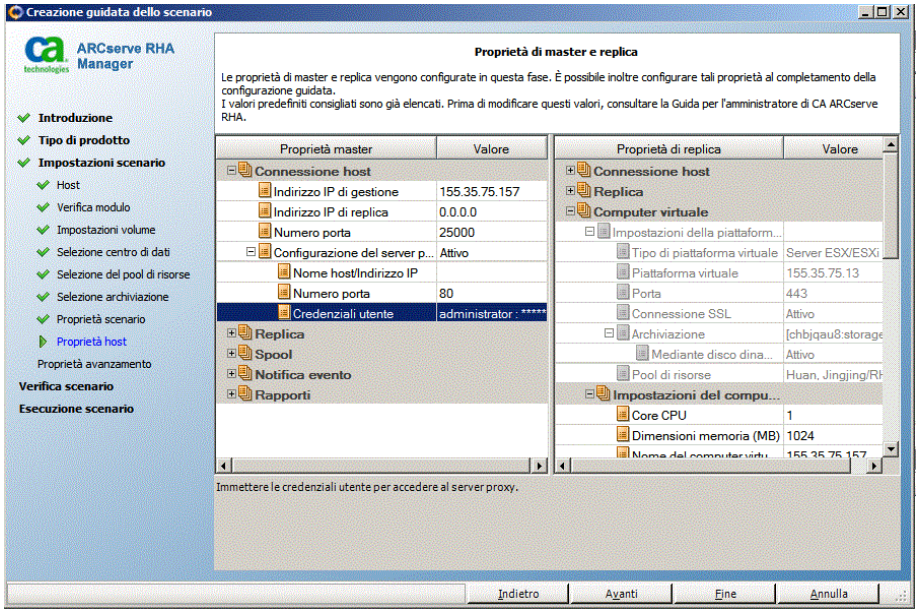


Questo esempio è simile all'Esempio 1. È sufficiente eseguire le fasi aggiuntive seguenti.

1. Sul master, specificare i seguenti dettagli del server proxy nell'utilità NAT.
   - **Server HTTP:** 155.35.76,123
   - **Porta:** 80
   - **Nome utente:** <dominio\nomeutente>
   - **Password:** <password>



2. Durante la creazione dello scenario di sistema completo, specificare le seguenti proprietà nella schermata Proprietà di master e replica.
   - Impostare la configurazione del server proxy HTTP su ON.
   - Immettere i dettagli del server proxy.

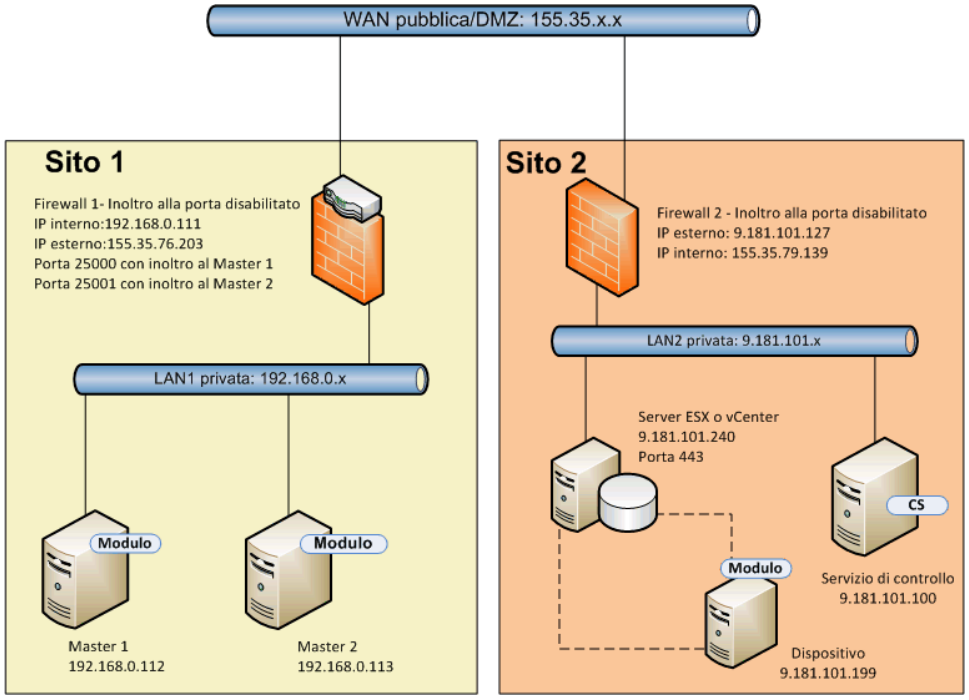


Esempio 3: Dispositivo e CS protetti da firewall chiuso

In questo esempio, il master non è in grado di accedere alla replica. Il Servizio di controllo e la replica sono protetti da firewall con l'inoltro alla porta disabilitato. Di seguito viene descritta l'impostazione di rete.

- I master sono inclusi in una rete LAN privata (LAN 1) protetta da firewall (Firewall 1) con l'inoltro alla porta abilitato.
- Gli host in LAN 1 sono in grado di accedere alla WAN pubblica mediante il Firewall 1. L'inoltro alla porta per il Firewall 1 è configurato nel seguente modo:
  - La porta 25000 esegue l'inoltro al Master 1.
  - La porta 25001 esegue l'inoltro al Master 2.
- Il Servizio di controllo e la replica sono inclusi in una rete LAN privata (LAN 2) protetta da firewall (Firewall2) senza inoltro alla porta.
- Entrambe le reti LAN private vengono connesse mediante una WAN pubblica.

Il seguente diagramma mostra l'impostazione di rete:



In questa impostazione, il Servizio di controllo e il dispositivo sono in grado di accedere al master, tuttavia il master non può accedere al dispositivo. In caso di scenario successivo, il master non sarà in grado di copiare i dati sulla replica.

Per creare uno scenario per questo tipo di impostazione, configurare l'utilità NAT per RHA sul dispositivo.

Di seguito si riportano le attività di configurazione dell'utilità NAT sul dispositivo durante la creazione di scenari e l'esecuzione del ripristino bare metal.

- Creazione di uno scenario HA per sistemi completi (a pagina 391)
- Esecuzione del ripristino bare metal da un punto di ripristino (a pagina 392)
- Esecuzione del ripristino bare metal mediante la replica inversa (a pagina 392)

Creazione di uno scenario HA per sistemi completi

Prima di creare lo scenario HA per sistemi completi, eseguire le operazioni seguenti sul dispositivo.

Procedere come descritto di seguito:

1. Avviare l'utilità NAT per RHA dalla cartella del modulo del dispositivo.
2. Immettere i seguenti indirizzi IP e i dettagli della porta.

   155.35.76.203, 25000
3. Fare clic su OK per applicare la configurazione.
4. Aprire la Gestione di RHA e fare clic su Nuovo sulla barra degli strumenti standard per creare lo scenario di sistema completo.
5. Selezionare Sistema completo e il tipo di prodotto, HA o AR.
6. Immettere l'indirizzo IP del Master (155.35.76.203) e il numero di porta (25000). Questo indirizzo IP corrisponde all'indirizzo IP esterno del Firewall 1 con porta 25000 e inoltro al Master 1 (192.168.0.112).
7. Immettere l'indirizzo IP (9.181.101.240) della piattaforma virtuale e il numero di porta predefinito (443).
8. Immettere l'indirizzo IP (9.181.101.199) del dispositivo e il numero di porta (25000).
9. Immettere dettagli del volume, del pool di risorse, dell'archiviazione, delle proprietà di scenario e delle proprietà host simili a quelli di uno scenario di sistema completo.
10. Selezionare il tipo di avanzamento ed eseguire lo scenario.

Esecuzione del ripristino bare metal da un punto di ripristino

Le operazioni da eseguire sono simili a quelle indicate nell'Esempio 1: Esecuzione del ripristino bare metal da un punto di ripristino. Solo le due operazioni seguenti si differenziano dall'Esempio 1.

- Dopo l'avvio del computer bare metal non è necessario configurare l'utilità NAT sul master. Il master esegue l'accesso al dispositivo mediante il Firewall 1 e l'inoltro alla porta.
- Nella pagina Destinazione di recupero, immettere il seguente indirizzo IP esterno del Firewall 1 e il numero della porta di inoltro.

  IP di destinazione: 155.35.76.203, 25000

Esecuzione del ripristino bare metal mediante la replica inversa

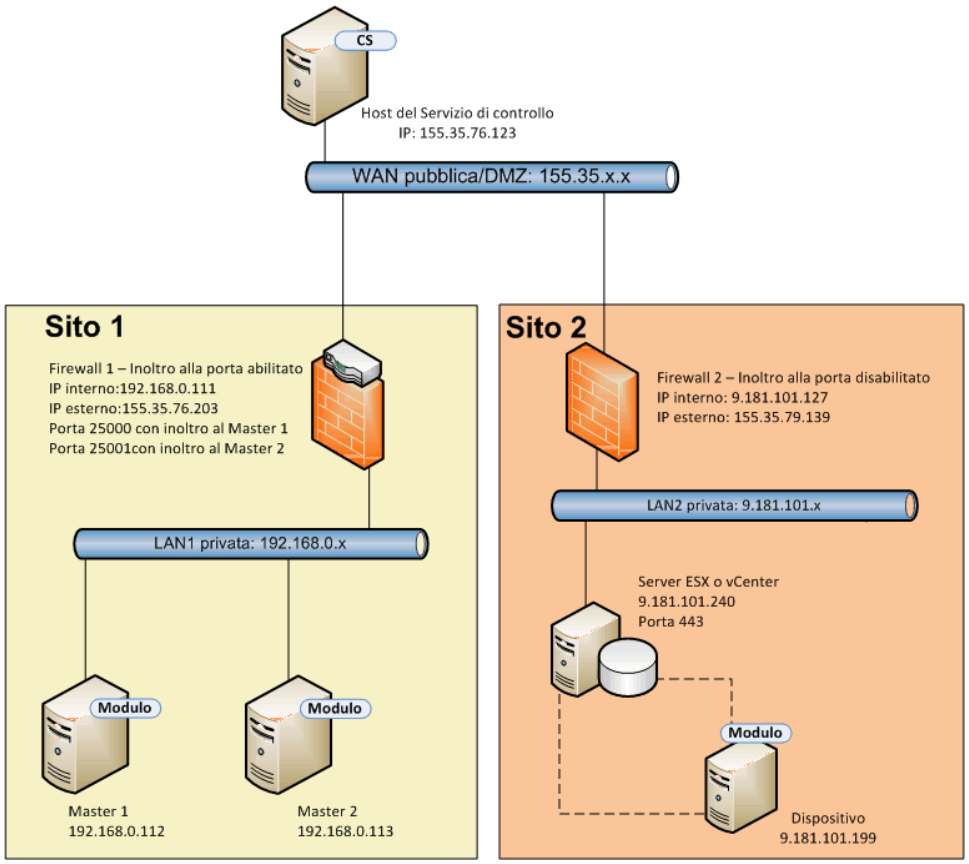
Durante l'avanzamento, il computer virtuale di avanzamento viene visualizzato come Sito 2. Questo computer virtuale di avanzamento è in grado di connettersi all'host in stand-by (Master 2) utilizzando l'indirizzo IP esterno e la l'inoltro alla porta del Firewall 1. In tal modo l'utilità NAT non è richiesta sul computer virtuale di avanzamento.

Esempio 4: Servizio di controllo su WAN pubblica

Questo esempio è simile all'Esempio 3 tranne per il fatto che l'host del Servizio di controllo è incluso in una WAN pubblica con un indirizzo IP pubblico (155.35.76.123). Di seguito viene descritta l'impostazione di rete.

- I master sono inclusi in una rete LAN privata (LAN 1) protetta da firewall (Firewall 1) con l'inoltro alla porta abilitato.
- Gli host in LAN 1 possono accedere alla WAN pubblica mediante il Firewall 1. L'inoltro alla porta per il Firewall 1 è configurato nel seguente modo:
  - La porta 25000 esegue l'inoltro al Master 1.
  - La porta 25001 esegue l'inoltro al Master 2.
- Il Servizio di controllo è in una WAN pubblica.
- Il dispositivo è incluso in una rete LAN privata (LAN 2) protetta da firewall (Firewall2) senza inoltro alla porta.
- Entrambe le reti LAN private vengono connesse mediante una WAN pubblica.

Il seguente diagramma mostra l'impostazione di rete:



Il Servizio di controllo è in grado di connettersi al master ma non al dispositivo. Configurare l'utilità NAT sul dispositivo per stabilire una connessione tra il Servizio di controllo e il master. Le altre fasi sono stesse come in Esempio 3.

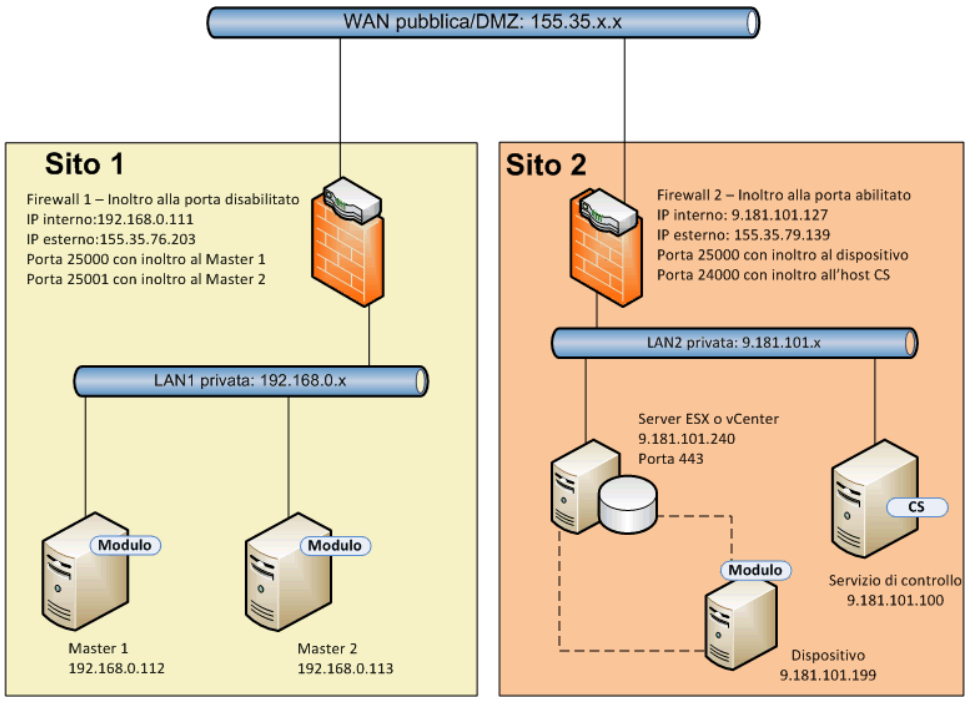
Esempio 5: Master, dispositivo e Servizio di controllo protetti da firewall con inoltro alla porta

Nel presente esempio, l'impostazione di rete prevede la protezione degli host di entrambi i siti mediante firewall con la funzione di inoltro alla porta abilitata.

Di seguito viene descritta l'impostazione di rete.

- I master sono inclusi in una rete LAN (LAN 1) protetta da firewall (Firewall 1).
- L'inoltro alla porta è abilitato per il Firewall 1.
- Il Servizio di controllo (CS) e la replica sono inclusi in una rete LAN (LAN 2) protetta da firewall (Firewall2).
- L'inoltro alla porta è abilitato per il Firewall 2.
- Entrambe le reti LAN utilizzano una WAN pubblica per la connessione.

Il diagramma seguente mostra l'impostazione di rete.



L'inoltro alla porta viene abilitato per entrambi i firewall, in modo tale da consentire ai master di accedere al dispositivo e al Servizio di controllo. Allo stesso modo, il Servizio di controllo e la replica possono accedere ai master Per questa impostazione, è possibile eseguire la creazione di uno scenario nei seguenti modi:

- **Mediante l'utilità NAT:** utilizzare l'utilità NAT sui master e sul dispositivo per creare uno scenario HA. Consultare l'Esempio 1 o l'Esempio 2.
- **Senza utilizzare l'utilità NAT:** per creare uno scenario HA, utilizzare gli indirizzi IP esterni di Firewall 1 e Firewall 2 con i dettagli di inoltro alla porta.

Appendice A: Risoluzione dei problemi di Arcserve RHA

Nella seguente sezione vengono fornite informazioni su alcuni dei messaggi di errore che potrebbero essere visualizzati: quando si verificano, il loro significato e come risolvere i problemi che li hanno originati.

Questa sezione contiene i seguenti argomenti:

Suggerimenti per la risoluzione dei problemi (a pagina 397)
Limite di spool superato (a pagina 398)
Disco pieno (a pagina 400)
EM03100 (a pagina 400)
EM03101 (a pagina 401)
EM03102 (a pagina 401)
EM03103 (a pagina 401)
Rinnovo di un certificato SSL scaduto (a pagina 402)
Impossibile iniziare l'ascolto sulla porta/e (a pagina 403)
Directory principali (a pagina 406)
Errore VSS durante la sincronizzazione (a pagina 407)
Errore di creazione della copia shadow (a pagina 407)
Errore di creazione della copia shadow per il punto di montaggio VHD (a pagina 408)

Suggerimenti per la risoluzione dei problemi

- Se viene attivato l'avanzamento manuale, Arcserve RHA invia l'ultimo evento di diario a tutti i nodi di replica prima dell'interruzione dello scenario. Quando il master è attivato, la sincronizzazione iniziale viene ignorata. Se si desidera eseguire la risincronizzazione forzata dal proprietario ad altri nodi, fare clic sull'opzione Eseguire la sincronizzazione forzata dei dati.
- Per ogni modifica di un nodo in un cluster (espulsione o aggiunta di un nodo), si consiglia di rianalizzare i nodi cluster per la risorsa. Per rianalizzare i nodi cluster, fare clic sull'opzione Ripeti analisi dei nodi cluster per la risorsa.

Limite di spool superato

CR00404 "Limite di spool superato.. Lo scenario verrà interrotto"

Motivo:

Questo messaggio può fare riferimento allo spool del master oppure allo spool della replica. Indica che il valore immesso in una delle proprietà di spool - **Dimensioni massime spool** o **Spazio libero su disco minimo -** è stato superato. Al raggiungimento della soglia il sistema genera un errore ed interrompe la replica in corso. Esiste un'eccezione a questa regola: quando il valore di **Dimensioni massime spool** sulla replica viene superato, viene generato un messaggio senza interrompere lo scenario. In questo caso viene visualizzato il seguente messaggio:**"ER00002" "Dimensione massima dello spool superata. Dimensione attuale: %1"**

L'aumento dello spool può essere determinato da vari fattori:

1. Sul master e sulla replica: durante una scansione antivirus in tempo reale vengono filtrati tutti i file replicati prima dell'applicazione della modifica ai file di dati. Con questo filtro i file replicati vengono memorizzati nella cache dello spool sul master e sulla replica, prima di essere trasferiti o applicati. Di conseguenza, viene visualizzato un collo di bottiglia ed è possibile superare il limite di spool.
2. Sul master: è possibile superare il limite di spool in caso di una connessione con larghezza di banda ridotta tra il master e la replica e un numero elevato di aggiornamenti sul master.
3. Sulla replica: se la sincronizzazione viene avviata durante l'esecuzione di una replica, i nuovi aggiornamenti provenienti dal master vengono archiviati sullo spool di replica. Solo al termine della sincronizzazione i file replicati memorizzati nella directory di spool vengono applicati ai dati di replica. Nel caso in cui la sincronizzazione richieda tempi lunghi o si verifichino numerose modifiche sul Master, il limite di spool potrebbe essere superato.
4. Sulla replica -- Durante la verifica Assured Recovery, le modifiche dei dati sul server master vengono inviate al server di replica, ma non vengono immediatamente applicate. Tali modifiche vengono piuttosto accumulate e archiviate in uno spool per essere applicate ai dati del server di replica solo al completamento della verifica. Ciò potrebbe determinare il superamento del limite di spool.
5. Sulla replica: se esiste un' attività elevata sulla directory dati del server di replica potrebbe formarsi una coda I/O sul disco. In questo modo i file replicati vengono memorizzati nella cache dello spool, in attesa di un accesso sequenziale al sottosistema del disco per poter applicare le modifiche dei dati ai file sul disco.
6. Esiste un elevato I/O su disco nella directory dati sul server di replica. Con l'operazione di I/O su disco la scrittura su disco viene messa in coda, e i file di replica vengono memorizzati nello spool, in attesa dell'accesso sequenziale al sottosistema di disco per l'applicazione delle modifiche ai dati dei file sul disco.

7. Per la risoluzione, eseguire i contatori delle prestazioni per effettuare la verifica di I/O su disco, oppure spostare lo spool su un volume con un I/O su disco relativamente basso. Non è consigliabile posizionare lo spool sullo stesso volume dei file di dati. Nel caso di un server applicazioni come Exchange, SQL, Oracle, ecc. lo spool non dove essere posizionato su un volume che contiene file di database o registri di transazione.

Nota:

- Nel caso di una disconnessione tra master e replica, lo spool del master che memorizza le modifiche applicate alla replica disconnessa verrà svuotato.
- Quando lo spool o l'unità di spool sono pieni, Arcserve RHA provvede all'interruzione dello scenario. Dopo aver riavviato lo scenario, lo spool viene svuotato e lo scenario può iniziare l'esecuzione. Tuttavia, se non vengono applicate modifiche alla definizione dello spool o all'unità di spool, il problema si verificherà nuovamente.

Azione:

È possibile eseguire una o tutte le azioni seguenti:

- Escludere la directory di spool di Arcserve RHA dall'analisi antivirus degli host coinvolti nella replica.
- Ridurre il valore immesso nella proprietà di**spool** - **Spazio libero su disco minimo** .
- Aumentare il valore immesso nella proprietà di **spool** - **Dimensioni massime spool** .
- Eseguire i contatori delle prestazioni per esaminare l'attività I/O su disco. Se necessario, modificare la posizione della **directory di spool** e selezionare un'unità libera e relativamente inattiva.

  Nota: si sconsiglia di posizionare lo spool Arcserve RHA sullo stesso volume dei file di dati. Nel caso di server di database come Exchange, SQL o Oracle, lo spool non deve essere posizionato su un volume contenente file di database o registri di transazione.
- Cancellare o spostare i file dall'unità di spool attuale, e ridurre le altre attività dello spool.

Disco pieno

"CR01488" "Disco pieno. Interruzione replica in corso"

Motivo:

Questo messaggio può fare riferimento sia al master che alla replica. Nella maggior parte dei casi fa riferimento a la mancanza di spazio libero sul disco sulla replica che impedisce alla replica di continuare.

L'esaurimento dello spazio sul disco di replica può essere determinato da diversi fattori comuni:

1. Se la dimensione dei dati replicati è superiore alla dimensione del disco della replica, questo risulterà pieno prima dell'applicazione di tutti i dati replicati.
2. Quando la replica contiene dati diversi, lo spazio libero potrebbe non essere sufficiente per memorizzare i dati replicati.
3. Se le snapshot VSS vengono create su base pianificata e archiviate sulla replica, queste potrebbero occupare troppo spazio sul disco.

Azione:

È possibile eseguire una o tutte le azioni seguenti:

- Liberare spazio sul disco pieno per i dati replicati.
- Controllare e confrontare la capacità di volume del disco della replica con la dimensione dei dati replicati, e selezionare un host di replica con sufficiente spazio libero sul disco
- Se il sistema è configurato per la creazione di snapshot VSS su base pianificata, è possibile rimuovere le snapshot precedenti o modificare la pianificazione e le proprietà delle snapshot VSS.

EM03100

Errore EM03100 La replica %1 non rientra nella distribuzione del master %2.

Applicabile a Dynamics CRM

Azione:

Reinstallare CRM sul server di replica e scegliere l'opzione per la connessione alla distribuzione esistente.

EM03101

Errore EM03101 I ruoli (salvo “SQL Server”) installati sulla replica sono diversi da quelli installati sul master. %1 %2

Applicabile a Dynamics CRM

Azione:

Installare gli stessi ruoli sia sul master che sulla replica.

EM03102

Errore EM03102 Ruolo '%1 non presente.

Applicabile a Dynamics CRM

Azione:

Installare gli stessi ruoli sul server master e sul server di replica.

EM03103

Errore EM03103 Ruolo '%1 ridondante.

Applicabile a Dynamics CRM

Azione:

Installare gli stessi ruoli sul server master e sul server di replica.

Rinnovo di un certificato SSL scaduto

Quando si utilizza un certificato SSL per proteggere le comunicazioni, potrebbe essere necessario rinnovare i certificati o installarne degli altri. La seguente procedura è applicabile a certificati SSL autorizzati e a certificati SSL autofirmati. Per ottenere un nuovo certificato, contattare il Supporto tecnico.

Per rinnovare un certificato SSL scaduto:

1. Ottenere un nuovo certificato ed installarlo sul computer un cui il Servizio di controllo è in esecuzione.

   Nota: non è necessario interrompere il Servizio di controllo durante questa fase.

2. Per rimuovere il binding del vecchio certificato, eseguire il seguente comando:

   `httpcfg.exe delete ssl -i 0,0.0,0:{CS SSL Port Number}`

   Il parametro numero di porta SSL del Servizio di controllo è il numero di porta immesso durante l'installazione del Servizio di controllo. È possibile rilevare il valore dal file ws_man.exe.config, sotto il valore ws_port.

   Il comando non dovrebbe restituire alcun errore.

   Il messaggio dovrebbe terminare con:
   `...completed with 0.`

3. Per eseguire il binding del nuovo certificato nella porta SSL del controllo di servizio, eseguire il seguente comando:
   `httpcfg.exe set ssl -i 0,0.0,0:{CS SSL Port Number} -h {New Certificate SslHash}`

   Il parametro httpcfg.exe è un'utilità standard per server Windows, reperibile nella directory di installazione del Servizio di controllo.

   È possibile trovare il parametro SSlHash del nuovo certificato nella finestra di dialogo Cerificato, nella scheda Dettagli, sotto il valore Thumbprint. Immettere il valore Thumbprint senza spazi, in un'unica stringa continua.

   Il comando non dovrebbe restituire alcun errore.

   Il messaggio dovrebbe terminare con:
   `...completed with 0.`

   Il certificato SSL è stato rinnovato.

Impossibile iniziare l'ascolto sulla porta/e

"CS00073" "Impossibile iniziare l'ascolto sulla porta %1 %%%"

Occupato o chiuso da un firewall (modulo).

"EM02012 Impossibile ottenere la porta del servizio Web su %1 %2"

Servizio di controllo occupato o chiuso da un firewall - 8088

"EM02014" Il Servizio di controllo ha una porta differente sugli host %1 %2 e %3 %4"

"ER00609" "Impossibile configurare la porta Web Access."

Scenario IIS -

Controllare se la porta è già utilizzata da un altro modulo o da un'altra applicazione. Modificare il numero di porta nel modulo oppure nell'applicazione.

Aprire le porte necessarie per l'installazione remota e per la verifica del modulo

Titolo: Elenco porte aperte necessarie per l'installazione remota e la verifica del modulo sugli host di replica.

Descrizione

Questo articolo indica le porte e i protocolli associati per l'installazione remota del servizio del modulo su host remoti attraverso la Creazione guidata scenario o l'installazione remota.

Soluzione

Le porte elencate di seguito dovranno essere aperte su tutti i firewall tra il server del Servizio di controllo di Arcserve RHA e i server del modulo.

- Il Protocollo CP richiede le porte 25000, 1025, 2666 e 2660
- Il Protocollo UDP richiede le porte 135, 137, e 138

Modifica della porta del Servizio di controllo

Per impostazione predefinita, il Servizio di controllo di Arcserve RHA prevede l'attesa sulla porta 8088. È possibile modificare la porta predefinita in ambienti in cui questa è già utilizzata da un'altra applicazione. Il file di configurazione responsabile della configurazione della porta del Servizio di controllo è ws_man.exe.config. Di conseguenza, se si desidera modificare la porta del Servizio di controllo dopo l'installazione, è necessario modificare tutti i valori della porta nel file ws_man.exe.config.

Modifica della porta predefinita del Servizio di controllo dalla porta 8088 a un'altra porta

1. Interrompere l'esecuzione degli scenari che utilizzano il Servizio di controllo che si desidera modificare mediante la Gestione di Arcserve RHA.
2. Collegarsi all'host in cui è in esecuzione il Servizio di controllo.
3. Nella finestra di dialogo **Servizi**, arrestare il Servizio di controllo.
4. Mediante Esplora risorse, accedere alla directory di installazione del Servizio di controllo dove si trova il file **ws_man.exe.config**.

   Note:

   - In un host a 32 bit, la directory di installazione predefinita è:"C:\Programmi\CA\Arcserve RHA\Manager"
   - In un host a 64 bit, la directory di installazione predefinita è: ""C:\Program Files (x86)\CA\Arcserve RHA\Manager"
5. Aprire il file **ws_man.exe.config** con un editor di testo.
6. Modificare il **valore** di tutte le voci '***_port**, ed immettere il numero di porta che si desidera utilizzare invece del numero 8088 corrispondente alla porta predefinita.
7. Salvare e chiudere il file **ws_man.exe.config**.
8. Nella finestra di dialogo **Servizi** , riavviare il Servizio di controllo. Il Servizio di controllo resta in attesa della nuova porta definita.

Modifica della porta del modulo

Il Modulo Arcserve RHA è stato progettato per impostazione predefinita per l'attesa sulla porta 25000. È possibile modificare la porta predefinita in ambienti in cui questa è già utilizzata da un'altra applicazione. Il file di configurazione responsabile della configurazione della porta è il file ws_rep.cfg. Di conseguenza, se si desidera modificare la porta del Servizio di controllo dopo l'installazione, è necessario modificare tutti i valori della porta nel file ws_rep.cfg.

Modifica del numero di porta utilizzato dal modulo di replica

1. Interrompere l'esecuzione degli scenari che utilizzano i moduli che si desidera modificare, utilizzando la Gestione di Arcserve RHA.
2. Accedere all'host master su cui il modulo è in esecuzione. (Ripetere il processo per la replica)
3. Nella finestra di dialogo **Servizi**, interrompere il servizio del **Modulo**. (Interrompere il modulo sul server master e sul server di replica.)
4. Mediante Esplora risorse, accedere alla directory di installazione del modulo, dove si trova il file **ws_rep.cfg**.

   Nota: La directory di installazione predefinita è la seguente: "C:\Programmi\CA\Arcserve RHA\Engine".
5. Aprire il file**ws_rep.cfg** con WordPad o con un altro editor di testo.

   Nota: Non è consigliabile utilizzare Blocco note, in quanto dispone di opzioni di visualizzazione limitate.
6. Il file WS_REP.CFG utilizza WordPad o un editor di testo di terze parti. (non utilizzare Blocco note).
7. Individuare la sezione "# Port = 25000" (una delle prime righe) nel file WS_REP.CFG.
8. Modificare la porta = 25000 con un nuovo numero di porta (per esempio porta = 25002) ed eliminare il simbolo # presente all'inizio della riga.
9. Salvare il file WS_REP.CFG. Attenzione: i file di configurazione sui server master e di replica devono coincidere. Assicurarsi che tutte le modifiche apportate al file WS_REP.CFG sul master vengano applicate anche al server di replica.
10. Avviare il servizio del modulo sia sul master che sulla replica.
11. Aprire la Gestione ed evidenziare lo scenario.
12. Fare clic sul server attivo, quindi scegliere Proprietà. Nella sezione di connessione, è viene visualizzato il numero di porta e il valore impostato su 25000. Modificare il numero di porta con il nuovo numero di porta specificato nel file WS_REP.CFG.
13. Ripetere le operazioni indicate nel passaggio 10 per il server di replica.
14. Se sono presenti altri scenari in esecuzione per i server master e di replica, sarà necessario modificarne il numero di porta.
15. Riavviare lo scenario.

Modifica della porta predefinita del Servizio di controllo dalla porta 8088 a un'altra porta

1. Collegarsi all'host in cui è in esecuzione il Servizio di controllo.
2. Nella finestra di dialogo **Servizi**, interrompere il Servizio di controllo.
3. Utilizzando Esplora risorse, accedere alla directory di installazione del Servizio di controllo in cui si trova il file **ws_man.exe.config**.

   Note:

   - In un host a 32 bit, il percorso di installazione predefinito è: "C:\Programmi\CA\Arcserve RHA\Manager"
   - In un host a 64 bit, il percorso predefinito è: "C:\Programmi (x86)\CA\Arcserve RHA\Manager"
4. Aprire il file **ws_man.exe.config** con un editor di testo.
5. Modificare il **valore** di tutte le voci ***_port** e immettere il numero di porta che si desidera utilizzare invece del numero 8088 corrispondente alla porta predefinita.
6. Salvare e chiudere il file **ws_man.exe.config**.

Nella finestra di dialogo **Servizi** riavviare il Servizio di controllo. Il Servizio di controllo resta in attesa della nuova porta definita.

Directory principali

"CV01361" Set directory principali non valido"

"EM00568 L'host %1 è già in uso dallo scenario HA '%2' in esecuzione'. "

L'host %1 è già in uso dallo scenario HA corrente '%2' in esecuzione.

Errore VSS durante la sincronizzazione

Sintomo:

Durante l'esecuzione della sincronizzazione viene visualizzato l'errore seguente:

```
WM04411 342 Avviso 155.35.86.133 10/09/12 17:17:00 Impossibile creare la copia
replicata. Nuovo tentativo in corso...
```

Soluzione:

Questo errore è causato da una configurazione hardware specifica. È possibile risolvere il problema eseguendo le operazioni seguenti:

Aprire ws_rep.cfg e modificare i parametri seguenti:

```
DirSnapshotWithVSS = True
MaxVSSRetryCount = 3
```

Nota: aumentare il valore di MaxVSSRetryCount se già impostato su 3.

Errore di creazione della copia shadow

Sintomo:

Durante l'esecuzione dello scenario viene visualizzato il seguente errore:

```
Impossibile creare la copia replicata, errore: Il sistema o il fornitore non
dispone di spazio sufficiente per l'archiviazione. Nuovo tentativo in corso...
```

Soluzione:

1. Aprire il file we_rep.cfg. abilitare il parametro SnapshotStorageVolume e impostarne il valore su un volume con spazio libero sufficiente.
2. Riavviare il modulo.
3. Eseguire nuovamente lo scenario.

Errore di creazione della copia shadow per il punto di montaggio VHD

Sintomo:

Non è possibile creare una copia shadow durante la sincronizzazione se il punto di montaggio VHD coesiste con altre directory come la directory principale.

Soluzione:

L'origine del problema potrebbe essere l'esistenza di più di una directory principale e la presenza delle directory in più di un volume. In questo caso, se alcuni dei volumi provengono da un file VHD, non è possibile eseguire lo scenario in quanto non è possibile creare un gruppo di copie shadow.

Per risolvere il problema, eseguire le seguenti operazioni:

1. Aprire ws_rep.cfg e modificare i parametri seguenti:

   ```
   DirSnapshotWithVSS = False
   ```

2. Eseguire nuovamente lo scenario.